Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 138, Task ID: 551

Task ID:	551
Risk Level:	7
Date Processed:	2016-04-28 13:01:58 (UTC)
Processing Time:	4.47 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\9b4316a022e8ffa53c35fafab8f7753b.exe"

Sample ID:	138
Type:	basic
Owner:	admin
Label:	9b4316a022e8ffa53c35fafab8f7753b
Date Added:	2016-04-28 12:45:04 (UTC)
File Type:	PE32:win32:gui
File Size:	305192 bytes
MD5:	9b4316a022e8ffa53c35fafab8f7753b
SHA256:	ff81ac1ada501179e980e72ae0459d6be9d6987581d867e79039f84ad8ebda54
Description:	None

Pattern Matching Results

- 2 PE: Nonstandard section
- 3 Long sleep detected
- 5 PE: Contains compressed section
- 6 Modifies registry autorun entries
- 5 Packer: UPX
- 4 Checks whether debugger is present
- 6 Installs service
- 7 Signed by adware producer [Adware, PUA]
- 7 Creates known events: Amonetize 2

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Packer:	UPX

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\9b4316a022e8ffa53c35fafab8f7753b.exe ["c:\windows\temp\9b4316a022e8ffa53c35fafab8f7753b.exe"]
Terminates process:	C:\WINDOWS\Temp\9b4316a022e8ffa53c35fafab8f7753b.exe

Named Object Events

Creates mutex:	\BaseNamedObjects\AmInst__Runing_1
Creates mutex:	\BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates event:	\BaseNamedObjects\AmiUpdInstallProgress
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Opens:	C:\WINDOWS\Prefetch\9B4316A022E8FFA53C35FAFAB8F77-0AD62E18.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\winhttp.dll
Opens:	C:\WINDOWS\system32\imm32.dll
Opens:	C:\WINDOWS\system32\shell32.dll
Opens:	C:\WINDOWS\system32\SHELL32.dll.124.Manifest
Opens:	C:\WINDOWS\system32\SHELL32.dll.124.Config
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens:	C:\WINDOWS\WindowsShell.Manifest
Opens:	C:\WINDOWS\WindowsShell.Config
Opens:	C:\WINDOWS\system32\comctl32.dll
Opens:	C:\WINDOWS\system32\comctl32.dll.124.Manifest
Opens:	C:\WINDOWS\system32\comctl32.dll.124.Config
Opens:	C:\Documents and Settings\Admin\Local Settings\Temp

```
  Opens:                  C:\WINDOWS\system32\rpcss.dll
  Opens:                  C:\WINDOWS\system32\iphlpapi.dll
  Opens:                  C:\WINDOWS\system32\ws2_32.dll
  Opens:                  C:\WINDOWS\system32\ws2help.dll
  Opens:                  C:\WINDOWS\system32\MSCTF.dll
  Opens:                  C:\WINDOWS\system32\clbcatq.dll
  Opens:                  C:\WINDOWS\system32\comres.dll
  Opens:                  C:\WINDOWS\Registration\R000000000007.clb
  Opens:                  C:\WINDOWS\system32\winlogon.exe
  Opens:                  C:\WINDOWS\system32\xpsp2res.dll
  Opens:                  C:\WINDOWS\system32\netman.dll
  Opens:                  C:\WINDOWS\system32\mprapi.dll
  Opens:                  C:\WINDOWS\system32\activeds.dll
  Opens:                  C:\WINDOWS\system32\adsldpc.dll
  Opens:                  C:\WINDOWS\system32\netapi32.dll
  Opens:                  C:\WINDOWS\system32\atl.dll
  Opens:                  C:\WINDOWS\system32\rtutils.dll
  Opens:                  C:\WINDOWS\system32\samlib.dll
  Opens:                  C:\WINDOWS\system32\setupapi.dll
  Opens:                  C:\WINDOWS\system32\netshell.dll
  Opens:                  C:\WINDOWS\system32\credui.dll
  Opens:                  C:\WINDOWS\system32\dot3api.dll
  Opens:                  C:\WINDOWS\system32\dot3dlg.dll
  Opens:                  C:\WINDOWS\system32\onex.dll
  Opens:                  C:\WINDOWS\system32\wtsapi32.dll
  Opens:                  C:\WINDOWS\system32\winsta.dll
  Opens:                  C:\WINDOWS\system32\crypt32.dll
  Opens:                  C:\WINDOWS\system32\msasn1.dll
  Opens:                  C:\WINDOWS\system32\eappcfg.dll
  Opens:                  C:\WINDOWS\system32\msvcp60.dll
  Opens:                  C:\WINDOWS\system32\eappprxy.dll
  Opens:                  C:\WINDOWS\system32\rasapi32.dll
  Opens:                  C:\WINDOWS\system32\rasman.dll
  Opens:                  C:\WINDOWS\system32\tapi32.dll
  Opens:                  C:\WINDOWS\system32\winmm.dll
  Opens:                  C:\WINDOWS\system32\wzcsapi.dll
  Opens:                  C:\WINDOWS\system32\wzcsvc.dll
  Opens:                  C:\WINDOWS\system32\wmi.dll
  Opens:                  C:\WINDOWS\system32\dhcpcsvc.dll
  Opens:                  C:\WINDOWS\system32\dnsapi.dll
  Opens:                  C:\WINDOWS\system32\eapolqec.dll
  Opens:                  C:\WINDOWS\system32\qutil.dll
  Opens:                  C:\WINDOWS\system32\esent.dll
  Opens:                  C:\WINDOWS\system32\netshell.dll.50.Manifest
  Opens:                  C:\WINDOWS\system32\netshell.dll.50.Config
  Opens:                  C:\WINDOWS\system32\TAPI32.dll.124.Manifest
  Opens:                  C:\WINDOWS\system32\TAPI32.dll.124.Config
  Opens:                  C:\WINDOWS\system32\urlmon.dll.123.Manifest
  Opens:                  C:\WINDOWS\system32\urlmon.dll.123.Config
  Opens:                  C:\WINDOWS\system32\WININET.dll.123.Manifest
  Opens:                  C:\WINDOWS\system32\WININET.dll.123.Config
  Reads from:             C:\WINDOWS\Registration\R000000000007.clb
```

Windows Registry Events

```
  Creates key:            HKLM\software\microsoft\windows nt\currentversion\tracing
  Creates key:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappcfg
  Creates key:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappcfg\traceidentifier
  Creates key:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappprxy
  Creates key:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappprxy\traceidentifier
  Creates key:            HKCU\software\microsoft\windows\currentversion\internet settings
  Creates key:            HKLM\system\currentcontrolset\services\tcpip\parameters
  Creates key:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qutil
  Creates key:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qutil\traceidentifier
  Creates key:            HKLM\software
  Creates key:            HKLM\software\microsoft
  Creates key:            HKLM\software\microsoft\esent
  Creates key:            HKLM\software\microsoft\esent\process
  Creates key:            HKLM\software\microsoft\esent\process\9b4316a022e8ffa53c35fafab8f7753b
  Creates key:
HKLM\software\microsoft\esent\process\9b4316a022e8ffa53c35fafab8f7753b\debug
  Creates key:            HKLM\system\currentcontrolset\services\eventlog\application\esent
  Creates key:            HKLM\software\microsoft\tracing
  Deletes value:
HKLM\software\microsoft\esent\process\9b4316a022e8ffa53c35fafab8f7753b\debug[trace level]
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\9b4316a022e8ffa53c35fafab8f7753b.exe
```

```
  Opens key:                HKLM\system\currentcontrolset\control\terminal server
  Opens key:                HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\secur32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\winlogon
  Opens key:                HKLM\
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\diagnostics
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\user32.dll
  Opens key:                HKLM\system\currentcontrolset\control\session manager
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntdll.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kernel32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcrt.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ole32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleaut32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shlwapi.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shell32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winhttp.dll
  Opens key:                HKLM\system\currentcontrolset\control\error message instrument\
  Opens key:                HKLM\system\currentcontrolset\control\error message instrument
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\gre_initialize
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\compatibility32
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\ime compatibility
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\windows
  Opens key:                HKLM\software\microsoft\ole
  Opens key:                HKCR\interface
  Opens key:                HKCR\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:                HKLM\software\microsoft\oleaut
  Opens key:                HKLM\software\microsoft\oleaut\userera
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer\performance
  Opens key:                HKLM\system\setup
  Opens key:                HKCU\
  Opens key:                HKCU\software\policies\microsoft\control panel\desktop
  Opens key:                HKCU\control panel\desktop
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comctl32.dll
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\languagepack
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\winhttp\tracing
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Opens key:                HKLM\software\microsoft\net framework setup\ndp\v1.1.4322
  Opens key:                HKLM\software\microsoft\net framework setup\ndp\v3.5
  Opens key:                HKLM\software\microsoft\net framework setup\ndp\v4\full
  Opens key:                HKLM\software\microsoft\net framework setup\ndp\v4\client
  Opens key:                HKLM\system\currentcontrolset\control\computername
  Opens key:                HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iphlpapi.dll
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\linkage
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\
  Opens key:                HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
  Opens key:                HKLM\system\currentcontrolset\services\netbt\parameters
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
  Opens key:
HKLM\software\microsoft\ctf\compatibility\9b4316a022e8ffa53c35fafab8f7753b.exe
```

```
  Opens key:               HKLM\software\microsoft\ctf\systemshared\
  Opens key:               HKCU\keyboard layout\toggle
  Opens key:               HKLM\software\microsoft\ctf\
  Opens key:               HKLM\software\microsoft\com3
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comres.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\clbcatq.dll
  Opens key:               HKLM\software\microsoft\com3\debug
  Opens key:               HKCU\software\classes\
  Opens key:               HKLM\software\classes
  Opens key:               HKU\
  Opens key:               HKCR\clsid
  Opens key:               HKCU\software\classes\clsid\{67bd9eeb-aa06-4329-a940-d250019300c9}
  Opens key:               HKCR\clsid\{67bd9eeb-aa06-4329-a940-d250019300c9}
  Opens key:               HKLM\software\microsoft\rpc\pagedbuffers
  Opens key:               HKLM\software\microsoft\rpc
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\9b4316a022e8ffa53c35fafab8f7753b.exe\rpcthreadpoolthrottle
  Opens key:               HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:               HKCU\software\classes\appid\9b4316a022e8ffa53c35fafab8f7753b.exe
  Opens key:               HKCR\appid\9b4316a022e8ffa53c35fafab8f7753b.exe
  Opens key:               HKLM\system\currentcontrolset\control\lsa
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}
  Opens key:               HKLM\software\microsoft\windows\currentversion\internet settings
  Opens key:               HKLM\software\microsoft\windows\currentversion\internet settings\winhttp
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netapi32.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wldap32.dll
  Opens key:               HKLM\system\currentcontrolset\services\ldap
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\adsldpc.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\atl.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\activeds.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rtutils.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\samlib.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\setupapi.dll
  Opens key:               HKLM\system\currentcontrolset\control\minint
  Opens key:               HKLM\system\wpa\pnp
  Opens key:               HKLM\software\microsoft\windows\currentversion\setup
  Opens key:               HKLM\software\microsoft\windows\currentversion
  Opens key:               HKLM\software\microsoft\windows\currentversion\setup\apploglevels
  Opens key:               HKLM\system\currentcontrolset\services\tcpip\parameters
  Opens key:               HKLM\software\policies\microsoft\system\dnsclient
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mprapi.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\credui.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dot3api.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winsta.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wtsapi32.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msasn1.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\crypt32.dll
  Opens key:               HKLM\system\currentcontrolset\services\crypt32\performance
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\msasn1
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcp60.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\eappcfg.dll
  Opens key:               HKLM\system\currentcontrolset\control\wmi\security
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\eappprxy.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\onex.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dot3dlg.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netshell.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasman.dll
```

```
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winmm.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\drivers32
  Opens key:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\tapi32.dll
  Opens key:                HKLM\software\microsoft\windows\currentversion\telephony
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasapi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\normaliz.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iertutil.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\urlmon.dll
  Opens key:                HKCU\software\classes\protocols\name-space handler\
  Opens key:                HKCR\protocols\name-space handler
  Opens key:                HKCU\software\classes\protocols\name-space handler
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\
  Opens key:                HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKLM\software\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKCU\software\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wininet.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wzcsapi.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dnsapi.dll
  Opens key:                HKLM\system\currentcontrolset\services\dnscache\parameters
  Opens key:                HKLM\software\policies\microsoft\windows nt\dnsclient
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dhcpcsvc.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\qutil.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\eapolqec.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\esent.dll
  Opens key:
HKLM\software\microsoft\esent\process\9b4316a022e8ffa53c35fafab8f7753b\debug
  Opens key:                HKLM\software\microsoft\esent\global\debug
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\connections
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wzcsvc.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netman.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\xpsp2res.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wmi.dll
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\winhttp\unsafesslapps
  Opens key:                HKLM\software\microsoft\tracing\rasapi32
  Opens key:                HKLM\system\currentcontrolset\control\network\{4d36e972-e325-11ce-bfc1-
08002be10318}\{16325b0b-4636-4303-abe3-c7d49d7cecdc}\connection
```

```
  Opens key:                HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\connections
  Opens key:                HKCU\software\classes\interface\{9edc0c90-2b5b-4512-953e-35767bad5c67}
  Opens key:                HKCR\interface\{9edc0c90-2b5b-4512-953e-35767bad5c67}
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
  Opens key:                HKLM\system\currentcontrolset\control\network\{4d36e972-e325-11ce-bfc1-
08002be10318}\{00000000-0000-0000-0000-000000000000}\connection
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\ms
tcp loopback interface
  Opens key:                HKLM\software\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\windows nt\currentversion
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
  Queries value:            HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\compatibility32[9b4316a022e8ffa53c35fafab8f7753b]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[9b4316a022e8ffa53c35fafab8f7753b]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
  Queries value:            HKLM\software\microsoft\ole[rwlockresourcetimeout]
  Queries value:            HKCR\interface[interfacehelperdisableall]
  Queries value:            HKCR\interface[interfacehelperdisableallforole32]
  Queries value:            HKCR\interface[interfacehelperdisabletypelib]
  Queries value:            HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableall]
  Queries value:            HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableallforole32]
  Queries value:            HKLM\system\setup[systemsetupinprogress]
  Queries value:            HKCU\control panel\desktop[multiuilanguageid]
  Queries value:            HKCU\control panel\desktop[smoothscroll]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[local appdata]
  Queries value:            HKLM\software\microsoft\net framework setup\ndp\v3.5[install]
  Queries value:            HKLM\software\microsoft\net framework setup\ndp\v3.5[version]
  Queries value:            HKLM\software\microsoft\net framework setup\ndp\v3.5[sp]
```

```
   Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
   Queries value:              HKLM\software\microsoft\ctf\systemshared[cuas]
   Queries value:              HKCU\keyboard layout\toggle[language hotkey]
   Queries value:              HKCU\keyboard layout\toggle[hotkey]
   Queries value:              HKCU\keyboard layout\toggle[layout hotkey]
   Queries value:              HKLM\software\microsoft\ctf[enableanchorcontext]
   Queries value:              HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
   Queries value:              HKLM\software\microsoft\com3[com+enabled]
   Queries value:              HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
   Queries value:              HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]
   Queries value:              HKLM\software\microsoft\com3[regdbversion]
   Queries value:              HKLM\software\microsoft\rpc[maxrpcsize]
   Queries value:              HKLM\software\microsoft\ole[maximumallowedallocationsize]
   Queries value:              HKLM\software\microsoft\ole[defaultaccesspermission]
   Queries value:              HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[enabledhcp]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[leaseobtainedtime]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[leaseterminatestime]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpserver]
   Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
   Queries value:              HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
   Queries value:              HKLM\system\wpa\pnp[seed]
   Queries value:              HKLM\system\setup[osloaderpath]
   Queries value:              HKLM\system\setup[systempartition]
   Queries value:              HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
   Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
   Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]
   Queries value:              HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
   Queries value:              HKLM\software\microsoft\windows\currentversion[devicepath]
   Queries value:              HKLM\software\microsoft\windows\currentversion\setup[loglevel]
   Queries value:              HKLM\software\microsoft\windows\currentversion\setup[logpath]
   Queries value:              HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
   Queries value:              HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
   Queries value:              HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
ab78-1084642581fb]
   Queries value:              HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
0000-000000000000]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
   Queries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
   Queries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32maxnumrequestretries]
   Queries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32requestretrytimeout]
   Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
   Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[9b4316a022e8ffa53c35fafab8f7753b.exe]
   Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
   Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
   Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
   Queries value:
```

```
HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
  Queries value:           HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
  Queries value:           HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
  Queries value:           HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
  Queries value:           HKLM\software\microsoft\esent\global\debug[trace level]
  Queries value:           HKLM\software\microsoft\windows\currentversion\internet
settings\connections[winhttpsettings]
  Queries value:           HKLM\software\microsoft\tracing[enableconsoletracing]
  Queries value:           HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
  Queries value:           HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
  Queries value:           HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
  Queries value:           HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
  Queries value:           HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
  Queries value:           HKLM\software\microsoft\tracing\rasapi32[filedirectory]
  Queries value:           HKLM\system\currentcontrolset\control\network\{4d36e972-e325-11ce-bfc1-
08002be10318}\{16325b0b-4636-4303-abe3-c7d49d7cecdc}\connection[name]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[domain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpdomain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registrationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registeradaptername]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Queries value:           HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[nameserver]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpnameserver]
   Queries value:            HKLM\software\microsoft\cryptography[machineguid]
   Queries value:            HKLM\software\microsoft\windows nt\currentversion[digitalproductid]
   Queries value:            HKLM\software\microsoft\windows nt\currentversion[digitalproductid4]
   Sets/Creates value:
HKLM\software\microsoft\esent\process\9b4316a022e8ffa53c35fafab8f7753b\debug[trace level]
   Value changes:            HKLM\software\microsoft\cryptography\rng[seed]
   Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappcfg[logsessionname]
   Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappcfg[active]
   Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappcfg[controlflags]
   Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappcfg\traceidentifier[guid]
   Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappcfg\traceidentifier[bitnames]
   Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappprxy[logsessionname]
   Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappprxy[active]
   Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappprxy[controlflags]
   Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappprxy\traceidentifier[guid]
```

```
  Value changes:             HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappprxy\traceidentifier[bitnames]
  Value changes:             HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qutil[logsessionname]
  Value changes:             HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qutil[active]
  Value changes:             HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qutil[controlflags]
  Value changes:             HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qutil\traceidentifier[guid]
  Value changes:             HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qutil\traceidentifier[bitnames]
  Value changes:
HKLM\system\currentcontrolset\services\eventlog\application\esent[eventmessagefile]
  Value changes:
HKLM\system\currentcontrolset\services\eventlog\application\esent[categorymessagefile]
  Value changes:
HKLM\system\currentcontrolset\services\eventlog\application\esent[categorycount]
  Value changes:
HKLM\system\currentcontrolset\services\eventlog\application\esent[typessupported]
```