Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	811
Risk Level:	3
Date Processed:	2016-04-28 13:09:53 (UTC)
Processing Time:	61.09 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\9a992314512bbc93b07328b3941fe048.exe"
Sample ID:	203
Type:	basic
Owner:	admin
Label:	9a992314512bbc93b07328b3941fe048
Date Added:	2016-04-28 12:45:11 (UTC)
File Type:	PE32:win32:gui
File Size:	925112 bytes
MD5:	9a992314512bbc93b07328b3941fe048
SHA256:	72668272001346e2deb5d2f4ff6836f7a6a613a25dfcf456c61ed1adc3ef03ef
Description:	None

Pattern Matching Results

`3` Writes to a log file [Info]

Static Events

Anomaly:	PE: Contains a virtual section

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\9a992314512bbc93b07328b3941fe048.exe

["c:\windows\temp\9a992314512bbc93b07328b3941fe048.exe"]

Named Object Events

Creates mutex:	\BaseNamedObjects\DirectSound DllMain mutex (0x000006A0)
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 mutex:	\BaseNamedObjects\RCPHost_Instance_Mutex
Creates event:	\BaseNamedObjects\EClientDisconnect45375
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Creates:	C:\WINDOWS\Temp\apc-host.log
Creates:	C:\WINDOWS\Temp\hostaccount.ini
Creates:	C:\WINDOWS\Temp\hoststate.dat
Opens:	C:\WINDOWS\Prefetch\9A992314512BBC93B07328B3941FE-0E9F36DA.pf
Opens:	C:\Documents and Settings\Admin
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\system32\winmm.dll
Opens:	C:\WINDOWS\system32\dsound.dll
Opens:	C:\WINDOWS\system32\wsock32.dll
Opens:	C:\WINDOWS\system32\ws2_32.dll
Opens:	C:\WINDOWS\system32\ws2help.dll
Opens:	C:\WINDOWS\system32\iphlpapi.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\WindowsShell.Manifest
Opens:	C:\WINDOWS\WindowsShell.Config
Opens:	C:\WINDOWS\Temp
Opens:	C:\WINDOWS\system32\MSCTF.dll
Opens:	C:\WINDOWS\system32\MSCTFIME.IME
Opens:	C:\
Opens:	C:\WINDOWS\Temp\apc-host.log
Opens:	C:\WINDOWS\system32\mswsock.dll

```
Opens:                    C:\WINDOWS\system32\hnetcfg.dll
Opens:                    C:\WINDOWS\system32\wshtcpip.dll
Opens:                    C:\WINDOWS\system32\dnsapi.dll
Opens:                    C:\WINDOWS\system32\winrnr.dll
Opens:                    C:\WINDOWS\system32\rasadhlp.dll
Opens:                    C:\windows\temp\hostaccount.ini
Opens:                    C:\WINDOWS\Temp\hostaccount.ini
Writes to:                C:\WINDOWS\Temp\apc-host.log
Writes to:                C:\WINDOWS\Temp\hostaccount.ini
Writes to:                C:\WINDOWS\Temp\hoststate.dat
Reads from:               C:\WINDOWS\Temp\hostaccount.ini
```

Windows Registry Events

```
Creates key:          HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\9a992314512bbc93b07328b3941fe048.exe
Opens key:            HKLM\system\currentcontrolset\control\terminal server
Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
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\gdi32.dll
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\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\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\version.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\comctl32.dll
Opens key:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winmm.dll
Opens key:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dsound.dll
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\wsock32.dll
Opens key:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iphlpapi.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\windows nt\currentversion\winlogon
Opens key:            HKLM\
Opens key:            HKLM\software\microsoft\windows nt\currentversion\diagnostics
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:              HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key:              HKLM\software\microsoft\windows nt\currentversion\languagepack
Opens key:              HKLM\software\microsoft\windows nt\currentversion\drivers32
Opens key:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
Opens key:              HKLM\software\microsoft\directx
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:              HKCU\software\borland\locales
Opens key:              HKLM\software\borland\locales
Opens key:              HKCU\software\borland\delphi\locales
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
Opens key:
HKLM\software\microsoft\ctf\compatibility\9a992314512bbc93b07328b3941fe048.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\windows nt\currentversion\imm
Opens key:              HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctfime.ime
Opens key:              HKCU\software\microsoft\ctf
Opens key:              HKLM\software\microsoft\ctf\systemshared
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:
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\software\microsoft\windows nt\currentversion\image file execution
options\mswsock.dll
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\hnetcfg.dll
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\9a992314512bbc93b07328b3941fe048.exe\rpcthreadpoolthrottle
Opens key:              HKLM\software\policies\microsoft\windows nt\rpc
Opens key:              HKLM\software\microsoft\rpc\securityservice
Opens key:              HKLM\system\currentcontrolset\services\winsock\parameters
Opens key:              HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wshtcpip.dll
```

```
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\dnsapi.dll
Opens key:              HKLM\system\currentcontrolset\services\dnscache\parameters
Opens key:              HKLM\software\policies\microsoft\windows nt\dnsclient
Opens key:              HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}
Opens key:              HKLM\software\policies\microsoft\system\dnsclient
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\winrnr.dll
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasadhlp.dll
Opens key:              HKCU\software\microsoft\multimedia\sound mapper
Opens key:              HKCU\software\microsoft\windows\currentversion\multimedia\midimap
Queries value:          HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
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[9a992314512bbc93b07328b3941fe048]
Queries value:          HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[9a992314512bbc93b07328b3941fe048]
Queries value:          HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
Queries value:          HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value:          HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
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:          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\directx[glitchinstrumentation]
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\software\microsoft\windows nt\currentversion\imm[ime file]
Queries value:          HKCU\software\microsoft\ctf[disable thread input manager]
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:
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\software\microsoft\rpc[maxrpcsize]
    Queries value:              HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
    Queries value:              HKLM\system\currentcontrolset\services\winsock\parameters[transports]
    Queries value:              HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
    Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
    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\system\currentcontrolset\services\tcpip\linkage[bind]
    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\system\currentcontrolset\services\tcpip\parameters[hostname]
    Queries value:               HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[queryadaptername]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[disableadapterdomainname]
    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\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registrationmaxaddresscount]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[maxnumberofaddressestoregister]
    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}[ipautoconfigurationenabled]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[addresstype]
```

```
    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\system\currentcontrolset\services\tcpip\parameters[searchlist]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
    Queries value:                HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
    Queries value:                HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
    Value changes:                HKLM\software\microsoft\cryptography\rng[seed]
```