Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	756
Risk Level:	10
Date Processed:	2016-05-18 10:34:15 (UTC)
Processing Time:	62.2 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\859ba9477553ccad1bba34c555ab6a1b.exe"

Sample ID:	3312
Type:	basic
Owner:	admin
Label:	859ba9477553ccad1bba34c555ab6a1b
Date Added:	2016-05-18 10:30:49 (UTC)
File Type:	PE32:win32:gui
File Size:	199680 bytes
MD5:	859ba9477553ccad1bba34c555ab6a1b
SHA256:	339ff6766efd4c5f26a8c0c9413b68ae664bb5eb8dfa403bec5df2909cbb73a1
Description:	None

Pattern Matching Results

6	Modifies registry autorun entries
7	Writes to memory of system processes
3	HTTP connection - response code 200 (success)
2	PE: Nonstandard section
5	Abnormal sleep detected
5	Installs service
7	Creates file in recycle bin
6	Changes Winsock providers
10	Creates malicious events: ZeroAccess [Rootkit]
4	Reads process memory
5	PE: Contains compressed section
7	Creates threads in system processes
7	Opens a recycle bin location
3	Long sleep detected
7	Injects thread into Windows process

Static Events

Anomaly:	PE: Contains one or more non-standard sections

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\859ba9477553ccad1bba34c555ab6a1b.exe ["c:\windows\temp\859ba9477553ccad1bba34c555ab6a1b.exe"]
Creates process:	C:\WINDOWS\system32\cmd.exe ["C:\WINDOWS\system32\cmd.exe"]
Reads from process:	PID:1728 C:\WINDOWS\system32\calc.exe
Writes to process:	PID:1904 C:\WINDOWS\explorer.exe
Writes to process:	PID:896 C:\WINDOWS\system32\services.exe
Writes to process:	PID:576 C:\WINDOWS\system32\cmd.exe
Terminates process:	C:\WINDOWS\Temp\859ba9477553ccad1bba34c555ab6a1b.exe
Creates remote thread:	C:\WINDOWS\explorer.exe
Creates remote thread:	C:\WINDOWS\system32\services.exe

Named Object Events

Creates mutex:	\BaseNamedObjects\SHIMLIB_LOG_MUTEX
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.EHH
Creates event:	\BaseNamedObjects\Restricted\{0C5AB9CD-2F90-6754-8374-21D4DAB28CC1}
Creates event:	\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D78}
Creates event:	\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D77}
Creates event:	\BaseNamedObjects\userenv: User Profile setup event
Creates event:	\BaseNamedObjects\CTF.ThreadMarshalInterfaceEvent.000007B8.00000000.00000004
Creates event:	\BaseNamedObjects\CTF.ThreadMIConnectionEvent.000007B8.00000000.00000004
Creates event:	\BaseNamedObjects\MSCTF.SendReceive.Event.ILH.IC
Creates event:	\BaseNamedObjects\MSCTF.SendReceiveConection.Event.ILH.IC
Creates event:	\BaseNamedObjects\MSCTF.SendReceive.Event.EHH.IC
Creates event:	\BaseNamedObjects\MSCTF.SendReceiveConection.Event.EHH.IC
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Creates:	C:\RECYCLER
Creates:	C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-1003
Creates:	C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-1003\$685c83111e534ea0f6bc8e25bc965f78
Creates:	C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-1003\$685c83111e534ea0f6bc8e25bc965f78\L
Creates:	C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-

```
1003\$685c83111e534ea0f6bc8e25bc965f78\U
  Creates:                    C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-
1003\$685c83111e534ea0f6bc8e25bc965f78\@
  Creates:                    C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-
1003\$685c83111e534ea0f6bc8e25bc965f78\n
  Creates:                    C:\RECYCLER\
  Creates:                    C:\RECYCLER\S-1-5-18
  Creates:                    C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78
  Creates:                    C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\L
  Creates:                    C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\U
  Creates:                    C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\@
  Creates:                    C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\n
  Creates:                    C:GAC_MSIL
  Creates:                    C:\WINDOWS\assembly\GAC
  Creates:                    C:\WINDOWS\assembly\GAC\Desktop.ini
  Opens:                      C:\WINDOWS\Prefetch\859BA9477553CCAD1BBA34C555AB6-0659C491.pf
  Opens:                      C:\Documents and Settings\Admin
  Opens:                      C:\WINDOWS\system32\atl.dll
  Opens:                      C:\WINDOWS\system32\imm32.dll
  Opens:                      C:\WINDOWS\system32\cabinet.dll
  Opens:                      C:\WINDOWS\system32\ws2_32.dll
  Opens:                      C:\WINDOWS\system32\ws2help.dll
  Opens:                      C:\WINDOWS\system32\mswsock.dll
  Opens:                      C:\WINDOWS\system32\hnetcfg.dll
  Opens:                      C:\WINDOWS\system32\wshtcpip.dll
  Opens:                      C:\WINDOWS\system32\rsaenh.dll
  Opens:                      C:\WINDOWS\system32\crypt32.dll
  Opens:                      C:\WINDOWS
  Opens:                      C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-
1003\$685c83111e534ea0f6bc8e25bc965f78
  Opens:                      C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-
1003\$685c83111e534ea0f6bc8e25bc965f78\n
  Opens:                      C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78
  Opens:                      C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\n
  Opens:                      C:\WINDOWS\assembly
  Opens:                      C:\WINDOWS\system32\cmd.exe
  Opens:                      C:\WINDOWS\system32\apphelp.dll
  Opens:                      C:\WINDOWS\AppPatch\sysmain.sdb
  Opens:                      C:\WINDOWS\AppPatch\systest.sdb
  Opens:                      C:\WINDOWS\system32
  Opens:                      C:\
  Opens:                      C:\WINDOWS\assembly\GAC\Desktop.ini
  Opens:                      C:\WINDOWS\assembly\GAC
  Opens:                      C:\WINDOWS\system32\cmd.exe.Manifest
  Opens:                      C:\WINDOWS\Temp\859ba9477553ccad1bba34c555ab6a1b.exe
  Opens:                      C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf
  Opens:                      C:
  Opens:                      C:\WINDOWS\AppPatch
  Opens:                      C:\WINDOWS\system32\wbem
  Opens:                      C:\WINDOWS\WinSxS
  Opens:                      C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
  Opens:                      C:\WINDOWS\system32\ntdll.dll
  Opens:                      C:\WINDOWS\system32\kernel32.dll
  Opens:                      C:\WINDOWS\system32\unicode.nls
  Opens:                      C:\WINDOWS\system32\locale.nls
  Opens:                      C:\WINDOWS\system32\sorttbls.nls
  Opens:                      C:\WINDOWS\system32\msvcrt.dll
  Opens:                      C:\WINDOWS\system32\user32.dll
  Opens:                      C:\WINDOWS\system32\gdi32.dll
  Opens:                      C:\WINDOWS\system32\shimeng.dll
  Opens:                      C:\WINDOWS\AppPatch\AcGenral.dll
  Opens:                      C:\WINDOWS\system32\advapi32.dll
  Opens:                      C:\WINDOWS\system32\rpcrt4.dll
  Opens:                      C:\WINDOWS\system32\secur32.dll
  Opens:                      C:\WINDOWS\system32\winmm.dll
  Opens:                      C:\WINDOWS\system32\ole32.dll
  Opens:                      C:\WINDOWS\system32\oleaut32.dll
  Opens:                      C:\WINDOWS\system32\msacm32.dll
  Opens:                      C:\WINDOWS\system32\version.dll
  Opens:                      C:\WINDOWS\system32\shell32.dll
  Opens:                      C:\WINDOWS\system32\shlwapi.dll
  Opens:                      C:\WINDOWS\system32\userenv.dll
  Opens:                      C:\WINDOWS\system32\uxtheme.dll
  Opens:                      C:\WINDOWS\system32\ctype.nls
  Opens:                      C:\WINDOWS\system32\sortkey.nls
  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\system32\comctl32.dll
  Opens:                      C:\WINDOWS\system32\wbem\wmic.exe
  Opens:                      C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\@
  Opens:                      C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-
```

```
1003\$685c83111e534ea0f6bc8e25bc965f78\@
  Opens:                    C:\WINDOWS\system32\SHELL32.dll.124.Manifest
  Opens:                    C:\WINDOWS\system32\SHELL32.dll.124.Config
  Opens:                    C:\WINDOWS\WindowsShell.Config
  Opens:                    C:\WINDOWS\system32\comctl32.dll.124.Manifest
  Opens:                    C:\WINDOWS\system32\comctl32.dll.124.Config
  Opens:                    C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\U
  Opens:                    C:\WINDOWS\Temp\100727f2-bbf4-4b86-92ba-5c99b64f3982
  Opens:                    C:\WINDOWS\system32\calc.exe
  Opens:                    C:\WINDOWS\system32\MSIMTF.dll
  Writes to:                C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-
1003\$685c83111e534ea0f6bc8e25bc965f78\@
  Writes to:                C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-
1003\$685c83111e534ea0f6bc8e25bc965f78\n
  Writes to:                C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\@
  Writes to:                C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\n
  Writes to:                C:\WINDOWS\assembly\GAC\Desktop.ini
  Reads from:               C:\WINDOWS\system32\rsaenh.dll
  Reads from:               C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf
  Reads from:               C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\@
  Reads from:               C:\WINDOWS\system32\calc.exe
  Deletes:                  C:\WINDOWS\Temp\859ba9477553ccad1bba34c555ab6a1b.exe
```

Network Events

```
  DNS query:                promos.fling.com
  DNS response:             promos.fling.com ⇒ 208.91.207.58
  Connects to:              208.91.207.58:80
  Connects to:              213.108.252.185:80
  Sends data to:            8.8.8.8:53
  Sends data to:            promos.fling.com:80 (208.91.207.58)
  Sends data to:            213.108.252.185:80
  Sends data to:            83.133.123.20:53
  Sends data to:            37.112.0.251:16471
  Sends data to:            68.104.123.244:16471
  Sends data to:            99.225.75.244:16471
  Sends data to:            94.240.212.241:16471
  Sends data to:            111.65.195.241:16471
  Sends data to:            184.66.166.241:16471
  Sends data to:            74.129.114.241:16471
  Sends data to:            70.176.247.237:16471
  Sends data to:            125.4.212.237:16471
  Sends data to:            94.24.192.232:16471
  Sends data to:            182.1.253.230:16471
  Sends data to:            87.3.88.229:16471
  Sends data to:            210.2.239.226:16471
  Sends data to:            71.62.37.224:16471
  Sends data to:            66.158.225.2:16471
  Sends data to:            69.242.115.222:16471
  Sends data to:            178.48.109.222:16471
  Sends data to:            83.14.18.222:16471
  Sends data to:            90.229.137.221:16471
  Sends data to:            219.173.240.2:16471
  Sends data to:            115.38.18.4:16471
  Sends data to:            72.48.52.8:16471
  Sends data to:            68.148.21.218:16471
  Sends data to:            46.237.125.216:16471
  Sends data to:            98.220.121.216:16471
  Sends data to:            89.214.82.216:16471
  Sends data to:            85.230.116.8:16471
  Sends data to:            173.19.154.215:16471
  Sends data to:            206.53.110.9:16471
  Sends data to:            142.167.122.9:16471
  Sends data to:            89.132.206.9:16471
  Sends data to:            75.131.172.213:16471
  Sends data to:            78.23.0.213:16471
  Sends data to:            186.10.14.10:16471
  Sends data to:            76.123.75.212:16471
  Sends data to:            113.211.35.11:16471
  Sends data to:            122.31.235.211:16471
  Sends data to:            46.128.24.13:16471
  Sends data to:            114.74.200.13:16471
  Sends data to:            87.1.83.15:16471
  Sends data to:            138.124.19.16:16471
  Sends data to:            121.84.80.16:16471
  Sends data to:            76.126.235.205:16471
  Sends data to:            69.143.155.205:16471
  Sends data to:            151.33.20.205:16471
  Sends data to:            93.171.119.17:16471
  Sends data to:            89.181.132.204:16471
  Sends data to:            24.222.98.204:16471
  Sends data to:            94.19.131.17:16471
  Sends data to:            65.31.38.203:16471
  Receives data from:     0.0.0.0:0
  Receives data from:     promos.fling.com:80 (208.91.207.58)
  Receives data from:     213.108.252.185:80
```

Windows Registry Events

```
  Creates key:            HKCU\software\classes\clsid
  Creates key:            HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}
  Creates key:            HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-
409d6c4515e9}\inprocserver32
  Creates key:            HKLM\software\clients\startmenuinternet
  Creates key:            HKCR\http\shell
  Creates key:            HKCU\software\microsoft\multimedia\audio
  Creates key:            HKCU\software\microsoft\multimedia\audio compression manager\
  Creates key:            HKCU\software\microsoft\multimedia\audio compression manager\msacm
  Creates key:            HKCU\software\microsoft\multimedia\audio compression manager\priority
v4.00
  Creates key:            HKCU\sessioninformation
  Deletes value:          HKLM\software\microsoft\windows\currentversion\run[windows defender]
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\859ba9477553ccad1bba34c555ab6a1b.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\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\msvcrt.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\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\shlwapi.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\windows\currentversion\explorer\performance
  Opens key:              HKCU\
  Opens key:              HKCU\software\policies\microsoft\control panel\desktop
  Opens key:              HKCU\control panel\desktop
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ole32.dll
  Opens key:              HKLM\software\microsoft\ole
  Opens key:              HKCR\interface
  Opens key:              HKCR\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cabinet.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\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\859ba9477553ccad1bba34c555ab6a1b.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\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rsaenh.dll
  Opens key:                HKLM\software\policies\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography\offload
  Opens key:                HKLM\software\microsoft\cryptography\deshashsessionkeybackward
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\shellserviceobjects\{fd6905ce-952f-41f1-
9a6f-135d9c6622cc}
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\shellserviceobjects\{f56f6fdd-aa9d-4618-
a949-c1b91af43b1a}
  Opens key:                HKLM\software\microsoft\windows\currentversion\run
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\n
  Opens key:                HKCU\software\classes\http
  Opens key:                HKCR\http
  Opens key:                HKCU\software\classes\http\curver
  Opens key:                HKCR\http\curver
  Opens key:                HKCR\http\
  Opens key:                HKCU\software\classes\http\shell\open
  Opens key:                HKCR\http\shell\open
  Opens key:                HKCU\software\classes\http\shell\open\command
  Opens key:                HKCR\http\shell\open\command
  Opens key:                HKCU\software\classes\http\shell
  Opens key:                HKLM\software\classes
  Opens key:                HKCU\software\classes\
  Opens key:                HKLM\software\microsoft\com3
  Opens key:                HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}
  Opens key:                HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}
  Opens key:                HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\treatas
  Opens key:                HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\treatas
  Opens key:                HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\inprocserver32
```

```
  Opens key:                 HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprocserver32
  Opens key:                 HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\inprocserverx86
  Opens key:                 HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprocserverx86
  Opens key:                 HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\localserver32
  Opens key:                 HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\localserver32
  Opens key:                 HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\inprochandler32
  Opens key:                 HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprochandler32
  Opens key:                 HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\inprochandlerx86
  Opens key:                 HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprochandlerx86
  Opens key:                 HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\localserver
  Opens key:                 HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\localserver
  Opens key:                 HKCU\software\classes\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}
  Opens key:                 HKCR\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}
  Opens key:                 HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}
  Opens key:                 HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}
  Opens key:                 HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\treatas
  Opens key:                 HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\treatas
  Opens key:                 HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\inprocserver32
  Opens key:                 HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserver32
  Opens key:                 HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\inprocserverx86
  Opens key:                 HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserverx86
  Opens key:                 HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\localserver32
  Opens key:                 HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\localserver32
  Opens key:                 HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\inprochandler32
  Opens key:                 HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprochandler32
  Opens key:                 HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\inprochandlerx86
  Opens key:                 HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprochandlerx86
  Opens key:                 HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\localserver
  Opens key:                 HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\localserver
  Opens key:                 HKCU\software\policies\microsoft\windows\network connections
  Opens key:                 HKLM\software\policies\microsoft\windows\network connections
  Opens key:                 HKCU\software\classes\clsid\{2227a280-3aea-1069-a2de-
08002b30309d}\shellfolder
  Opens key:                 HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}\shellfolder
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\clsid\{2227a280-
3aea-1069-a2de-08002b30309d}
  Opens key:                 HKCU\software\microsoft\windows\currentversion\policies\nonenum
  Opens key:                 HKLM\software\microsoft\windows\currentversion\policies\nonenum
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{2227a280-3aea-1069-
a2de-08002b30309d}
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\clsid\{2227a280-
3aea-1069-a2de-08002b30309d}\shellfolder
  Opens key:                 HKLM\software\microsoft\windows\currentversion\explorer\clsid\{2227a280-
3aea-1069-a2de-08002b30309d}\shellfolder
  Opens key:                 HKCU\software\classes\clsid\{2227a280-3aea-1069-a2de-08002b30309d}
  Opens key:                 HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}
  Opens key:                 HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}\
  Opens key:                 HKCU\software\microsoft\windows\shellnoroam\muicache\
  Opens key:                 HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}\shellfolder
  Opens key:                 HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\shellfolder
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\clsid\{7007acc7-
3202-11d1-aad2-00805fc1270e}
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{7007acc7-3202-11d1-
aad2-00805fc1270e}
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\clsid\{7007acc7-
3202-11d1-aad2-00805fc1270e}\shellfolder
  Opens key:                 HKLM\software\microsoft\windows\currentversion\explorer\clsid\{7007acc7-
3202-11d1-aad2-00805fc1270e}\shellfolder
  Opens key:                 HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}
  Opens key:                 HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}
  Opens key:                 HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\
  Opens key:                 HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32
  Opens key:                 HKLM\system\currentcontrolset\control\session manager\appcertdlls
  Opens key:                 HKLM\system\currentcontrolset\control\session manager\appcompatibility
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\apphelp.dll
  Opens key:                 HKLM\system\wpa\tabletpc
  Opens key:                 HKLM\system\wpa\mediacenter
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:              HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\cmd.exe
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\appcompatflags
  Opens key:              HKCU\software\microsoft\windows nt\currentversion\appcompatflags
  Opens key:              HKLM\software\policies\microsoft\windows\safer\levelobjects
  Opens key:              HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}
  Opens key:              HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
  Opens key:              HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
  Opens key:              HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
```

```
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cmd.exe
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\acgenral.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shimeng.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\oleaut32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msacm32.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\userenv.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.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\oleaut
  Opens key:                HKLM\software\microsoft\oleaut\userera
  Opens key:                HKLM\software\microsoft\audiocompressionmanager\drivercache
  Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm
  Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm
  Opens key:                HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711
  Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610
  Opens key:                HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch
  Opens key:                HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723
  Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1
  Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet
  Opens key:                HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2
  Opens key:                HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm
  Opens key:                HKLM\system\currentcontrolset\control\mediaresources\acm
  Opens key:                HKLM\system\setup
  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\system\currentcontrolset\control\productoptions
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Opens key:                HKLM\software\policies\microsoft\windows\system
  Opens key:                HKCU\software\microsoft\windows\currentversion\thememanager
  Opens key:                HKLM\system\currentcontrolset\services\sharedaccess
  Opens key:                HKCU\software\classes\applications\calc.exe
  Opens key:                HKCR\applications\calc.exe
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer\fileassociation
  Opens key:                HKLM\software\microsoft\ctf\tip\
  Opens key:                HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}
  Opens key:                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}
  Opens key:                HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}
  Opens key:                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}
  Opens key:                HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
  Opens key:                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
  Opens key:                HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
  Opens key:                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
  Opens key:                HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}
  Opens key:                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}
  Opens key:                HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
  Opens key:                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
  Opens key:                HKCU\appevents\schemes\apps\.default\systemnotification\.current
```

```
   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[859ba9477553ccad1bba34c555ab6a1b]
   Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[859ba9477553ccad1bba34c555ab6a1b]
   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:            HKCU\control panel\desktop[multiuilanguageid]
   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\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\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0[type]
  Queries value:            HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0[image path]
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  Queries value:            HKLM\software\microsoft\cryptography[machineguid]
  Queries value:            HKCR\http\shell\open\command[]
  Queries value:            HKLM\software\clients\startmenuinternet[]
  Queries value:            HKLM\software\microsoft\com3[regdbversion]
  Queries value:            HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}[appid]
  Queries value:            HKCR\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}[dllsurrogate]
  Queries value:            HKCR\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}[localservice]
  Queries value:            HKCR\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserver32[]
  Queries value:            HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}[appid]
  Queries value:            HKCR\clsid\{2227a280-3aea-1069-a2de-
08002b30309d}\shellfolder[wantsfordisplay]
  Queries value:            HKCR\clsid\{2227a280-3aea-1069-a2de-
08002b30309d}\shellfolder[attributes]
  Queries value:            HKCR\clsid\{2227a280-3aea-1069-a2de-
08002b30309d}\shellfolder[callforattributes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{2227a280-3aea-1069-a2de-
08002b30309d}]
  Queries value:            HKCR\clsid\{2227a280-3aea-1069-a2de-
08002b30309d}\shellfolder[hidefolderverbs]
  Queries value:            HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}[localizedstring]
  Queries value:
HKCU\software\microsoft\windows\shellnoroam\muicache[@c:\windows\system32\shell32.dll,-9319]
  Queries value:            HKCR\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}\shellfolder[wantsfordisplay]
  Queries value:            HKCR\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}\shellfolder[attributes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{7007acc7-3202-11d1-aad2-
00805fc1270e}]
  Queries value:            HKCR\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}\shellfolder[hidefolderverbs]
  Queries value:            HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[localizedstring]
  Queries value:
```

```
HKCU\software\microsoft\windows\shellnoroam\muicache[@c:\windows\system32\netshell.dll,-1200]
   Queries value:              HKLM\system\currentcontrolset\control\session
manager\appcompatibility[disableappcompat]
   Queries value:              HKLM\system\wpa\mediacenter[installed]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[current_protocol_catalog]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[current_namespace_catalog]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
   Queries value:              HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}[itemdata]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemdata]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[hashalg]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemsize]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[itemdata]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[hashalg]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[itemsize]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemdata]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[hashalg]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemsize]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemdata]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[hashalg]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemsize]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemdata]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[hashalg]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemsize]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
   Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
```

```
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\compatibility32[cmd]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime compatibility[cmd]
  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:            HKCU\software\microsoft\multimedia\audio[systemformats]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.imaadpcm]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[fdwsupport]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[aformattagcache]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cfiltertags]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msadpcm]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[fdwsupport]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cformattags]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[aformattagcache]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cfiltertags]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msg711]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[fdwsupport]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cformattags]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[aformattagcache]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cfiltertags]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msgsm610]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[fdwsupport]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cformattags]
```

```
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[aformattagcache]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cfiltertags]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.trspch]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cformattags]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[aformattagcache]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cfiltertags]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msg723]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[fdwsupport]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cformattags]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[aformattagcache]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cfiltertags]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msaudio1]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[fdwsupport]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cformattags]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[aformattagcache]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cfiltertags]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.sl_anet]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[fdwsupport]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cformattags]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[aformattagcache]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cfiltertags]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cformattags]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[aformattagcache]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cfiltertags]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.l3acm]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[fdwsupport]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cformattags]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[aformattagcache]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags]
  Queries value:            HKCU\software\microsoft\multimedia\audio compression
manager\msacm[nopcmconverter]
  Queries value:            HKCU\software\microsoft\multimedia\audio compression manager\priority
v4.00[priority1]
  Queries value:            HKLM\system\setup[systemsetupinprogress]
  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\winlogon[userenvdebuglevel]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\winlogon[chkaccdebuglevel]
  Queries value:            HKLM\system\currentcontrolset\control\productoptions[producttype]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[personal]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local settings]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\winlogon[rsopdebuglevel]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
  Queries value:            HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
```

```
   Queries value:               HKCU\control panel\desktop[lamebuttontext]
   Queries value:               HKLM\system\currentcontrolset\services\sharedaccess[start]
   Queries value:
HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\calc.exe]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\fileassociation[cutlist]
   Queries value:               HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}[dword]
   Queries value:               HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}[dword]
   Queries value:               HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}[dword]
   Queries value:               HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[dword]
   Queries value:               HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}[dword]
   Queries value:               HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}[dword]
   Queries value:               HKCU\appevents\schemes\apps\.default\systemnotification\.current[]
   Sets/Creates value:          HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-
409d6c4515e9}\inprocserver32[threadingmodel]
   Sets/Creates value:          HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-
409d6c4515e9}\inprocserver32[]
   Sets/Creates value:
HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\calc.exe]
   Value changes:               HKLM\software\microsoft\cryptography\rng[seed]
   Value changes:               HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32[]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
   Value changes:               HKCU\sessioninformation[programcount]
```