Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3329, Task ID: 824

Task ID:	824
Risk Level:	10
Date Processed:	2016-05-18 10:42:22 (UTC)
Processing Time:	62.47 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\26ec828da6d2651f90c74cb275b800cc.exe"

Sample ID:	3329
Type:	basic
Owner:	admin
Label:	26ec828da6d2651f90c74cb275b800cc
Date Added:	2016-05-18 10:30:51 (UTC)
File Type:	PE32:win32:gui
File Size:	184320 bytes
MD5:	26ec828da6d2651f90c74cb275b800cc
SHA256:	2fd94a7ba79df111cbd03365c4ae7ccc17e7dfaba10a30ed3049db2f369c2d4b
Description:	None

Pattern Matching Results

7	Writes to memory of system processes
6	Modifies registry autorun entries
5	Abnormal sleep detected
5	Installs service
10	Creates malicious events: ZeroAccess [Rootkit]
7	Creates file in recycle bin
6	Changes Winsock providers
3	Connects to local host
4	Reads process memory
7	Opens a recycle bin location
7	Creates threads in system processes
3	Long sleep detected
7	Injects thread into Windows process

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\26ec828da6d2651f90c74cb275b800cc.exe ["c:\windows\temp\26ec828da6d2651f90c74cb275b800cc.exe"]
Reads from process:	PID:1900 C:\WINDOWS\Temp\26ec828da6d2651f90c74cb275b800cc.exe
Reads from process:	PID:1112 C:\WINDOWS\system32\calc.exe
Writes to process:	PID:1900 C:\WINDOWS\Temp\26ec828da6d2651f90c74cb275b800cc.exe
Writes to process:	PID:1984 C:\WINDOWS\explorer.exe
Writes to process:	PID:896 C:\WINDOWS\system32\services.exe
Terminates process:	C:\WINDOWS\Temp\26ec828da6d2651f90c74cb275b800cc.exe
Creates remote thread:	C:\WINDOWS\explorer.exe
Creates remote thread:	C:\WINDOWS\system32\services.exe

Named Object Events

Creates mutex:	\BaseNamedObjects\DDrawWindowListMutex
Creates mutex:	\BaseNamedObjects__DDrawExclMode__
Creates mutex:	\BaseNamedObjects__DDrawCheckExclMode__
Creates mutex:	\BaseNamedObjects\DDrawDriverObjectListMutex
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.EMH
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\CTF.ThreadMarshalInterfaceEvent.000000E4.00000000.00000004
Creates event:	\BaseNamedObjects\CTF.ThreadMIConnectionEvent.000000E4.00000000.00000004
Creates event:	\BaseNamedObjects\MSCTF.SendReceive.Event.EO.IC
Creates event:	\BaseNamedObjects\MSCTF.SendReceiveConection.Event.EO.IC
Creates event:	\BaseNamedObjects\MSCTF.SendReceive.Event.EMH.IC
Creates event:	\BaseNamedObjects\MSCTF.SendReceiveConection.Event.EMH.IC

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:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-1003\$I5D1DD46B
  Creates:                C:GAC_MSIL
  Creates:                C:\WINDOWS\assembly\GAC
  Creates:                C:\WINDOWS\assembly\GAC\Desktop.ini
  Opens:                  C:\WINDOWS\Prefetch\26EC828DA6D2651F90C74CB275B80-349933DF.pf
  Opens:                  C:\Documents and Settings\Admin
  Opens:                  C:\WINDOWS\system32\d3d8.dll
  Opens:                  C:\WINDOWS\system32\d3d8thk.dll
  Opens:                  C:\WINDOWS\system32\opengl32.dll
  Opens:                  C:\WINDOWS\system32\glu32.dll
  Opens:                  C:\WINDOWS\system32\ddraw.dll
  Opens:                  C:\WINDOWS\system32\dciman32.dll
  Opens:                  C:\WINDOWS\system32\imm32.dll
  Opens:                  C:\WINDOWS\win.ini
  Opens:                  C:\WINDOWS\Temp\26ec828da6d2651f90c74cb275b800cc.exe
  Opens:                  C:\WINDOWS\system32\mscat32.dll
  Opens:                  C:\WINDOWS\system32\wintrust.dll
  Opens:                  C:\WINDOWS\system32\crypt32.dll
  Opens:                  C:\WINDOWS\system32\msasn1.dll
  Opens:                  C:\WINDOWS\system32\apphelp.dll
  Opens:                  C:\WINDOWS\AppPatch\sysmain.sdb
  Opens:                  C:\WINDOWS\AppPatch\systest.sdb
  Opens:                  C:\WINDOWS\Temp
  Opens:                  C:\
  Opens:                  C:\WINDOWS
  Opens:                  C:\windows\temp\26ec828da6d2651f90c74cb275b800cc.exe.Manifest
  Opens:                  C:\WINDOWS\system32\ntdll.dll
  Opens:                  C:\WINDOWS\system32\kernel32.dll
  Opens:                  C:\WINDOWS\system32\user32.dll
  Opens:                  C:\WINDOWS\system32\gdi32.dll
  Opens:                  C:\WINDOWS\system32\msvcrt.dll
  Opens:                  C:\WINDOWS\system32\advapi32.dll
  Opens:                  C:\WINDOWS\system32\rpcrt4.dll
  Opens:                  C:\WINDOWS\system32\secur32.dll
  Opens:                  C:\WINDOWS\system32\version.dll
  Opens:                  C:\WINDOWS\system32\imagehlp.dll
  Opens:                  C:\WINDOWS\system32\untfs.dll
  Opens:                  C:\WINDOWS\system32\cabinet.dll
  Opens:                  C:\WINDOWS\system32\ole32.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:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-
1003\$685c83111e534ea0f6bc8e25bc965f78
  Opens:                  C:\Program Files\Windows Defender
  Opens:                  C:\Program Files\Microsoft Security Client
  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:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-1003
  Opens:                  C:\WINDOWS\Temp\c76432ab-d183-41af-8e59-0ccaef29b5ae
  Opens:                  C:\WINDOWS\assembly
  Opens:                  C:\WINDOWS\assembly\GAC\Desktop.ini
  Opens:                  C:\WINDOWS\assembly\GAC
  Opens:                  C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\@
  Opens:                  C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-
1003\$685c83111e534ea0f6bc8e25bc965f78\@
  Opens:                  C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\U
  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:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-1003\$I5D1DD46B
  Writes to:              C:\WINDOWS\assembly\GAC\Desktop.ini
  Reads from:             C:\WINDOWS\win.ini
  Reads from:             C:\WINDOWS\Temp\26ec828da6d2651f90c74cb275b800cc.exe
  Reads from:             C:\WINDOWS\system32\rsaenh.dll
  Reads from:             C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\@
```

Reads from:	C:\WINDOWS\system32\calc.exe
Deletes:	C:\WINDOWS\Temp\26ec828da6d2651f90c74cb275b800cc.exe

Network Events

DNS query:	j.maxmind.com
DNS response:	j.maxmind.com ⇒ 127.0.0.1
Connects to:	127.0.0.1:80
Sends data to:	8.8.8.8:53
Sends data to:	83.133.123.20:53
Sends data to:	206.254.253.254:16471
Sends data to:	197.254.253.254:16471
Sends data to:	190.254.253.254:16471
Sends data to:	184.254.253.254:16471
Sends data to:	183.254.253.254:16471
Sends data to:	182.254.253.254:16471
Sends data to:	180.254.253.254:16471
Sends data to:	166.254.253.254:16471
Sends data to:	158.254.253.254:16471
Sends data to:	135.254.253.254:16471
Sends data to:	134.254.253.254:16471
Sends data to:	119.254.253.254:16471
Sends data to:	117.254.253.254:16471
Sends data to:	115.254.253.254:16471
Sends data to:	113.254.253.254:16471
Sends data to:	97.85.204.165:16471
Sends data to:	75.196.193.163:16471
Sends data to:	174.126.150.143:16471
Sends data to:	123.98.238.25:16471
Sends data to:	84.201.207.181:16471
Sends data to:	2.191.103.138:16471
Sends data to:	81.185.121.132:16471
Sends data to:	77.52.137.124:16471
Sends data to:	78.88.111.189:16471
Sends data to:	82.182.148.121:16471
Sends data to:	75.201.223.242:16471
Sends data to:	37.214.60.116:16471
Sends data to:	60.251.49.107:16471
Sends data to:	98.225.26.239:16471
Sends data to:	79.118.247.238:16471
Sends data to:	70.83.137.237:16471
Sends data to:	184.191.56.101:16471
Sends data to:	123.0.235.46:16471
Sends data to:	66.176.166.98:16471
Sends data to:	67.78.102.59:16471
Sends data to:	111.240.114.96:16471
Sends data to:	70.135.92.66:16471
Sends data to:	98.155.179.82:16471
Sends data to:	2.179.94.81:16471
Sends data to:	85.120.81.68:16471
Sends data to:	85.196.244.71:16471
Sends data to:	176.10.223.172:16471
Sends data to:	95.76.9.80:16471
Sends data to:	85.122.52.77:16471
Sends data to:	122.149.32.73:16471
Sends data to:	186.89.188.215:16471
Sends data to:	76.190.181.221:16471
Sends data to:	213.91.131.223:16471
Sends data to:	67.84.253.87:16471
Sends data to:	153.180.226.90:16471
Sends data to:	86.105.88.95:16471
Sends data to:	188.24.98.227:16471
Sends data to:	67.250.72.51:16471
Receives data from:	0.0.0.0:0

Windows Registry Events

Creates key:	HKLM\software\microsoft\direct3d\mostrecentapplication
Creates key:	HKLM\software\microsoft\directdraw\mostrecentapplication
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\sessioninformation
Deletes value:	HKLM\software\microsoft\windows\currentversion\run[windows defender]
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\26ec828da6d2651f90c74cb275b800cc.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\d3d8thk.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\version.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\d3d8.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\glu32.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dciman32.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ddraw.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\opengl32.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\direct3d
  Opens key:               HKLM\hardware\devicemap\video
  Opens key:               HKLM\software\microsoft\directdraw\compatibility
  Opens key:               HKLM\software\microsoft\directdraw\compatibility\bug!
  Opens key:               HKLM\software\microsoft\directdraw\compatibility\demolitionderby2
  Opens key:               HKLM\software\microsoft\directdraw\compatibility\mortalkombat3
  Opens key:               HKLM\software\microsoft\directdraw\compatibility\msgolf98
  Opens key:               HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay
  Opens key:               HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo
  Opens key:               HKLM\software\microsoft\directdraw\compatibility\rogue squadron
  Opens key:               HKLM\software\microsoft\directdraw\compatibility\savage
  Opens key:               HKLM\software\microsoft\directdraw\compatibility\scorchedplanet
  Opens key:               HKLM\software\microsoft\directdraw\compatibility\silentthunder
  Opens key:               HKLM\software\microsoft\directdraw\compatibility\terracide
  Opens key:               HKLM\software\microsoft\directdraw\compatibility\thirddimension
  Opens key:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark
  Opens key:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark
  Opens key:               HKLM\software\microsoft\directdraw\gammacalibrator
  Opens key:               HKLM\software\microsoft\directdraw
  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\msasn1.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\crypt32.dll
  Opens key:               HKLM\system\currentcontrolset\services\crypt32\performance
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\msasn1
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imagehlp.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wintrust.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mscat32.dll
  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\26ec828da6d2651f90c74cb275b800cc.exe
  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\software\microsoft\windows nt\currentversion\image file execution
options\untfs.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\26ec828da6d2651f90c74cb275b800cc.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\system\currentcontrolset\services\windefend
  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\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[26ec828da6d2651f90c74cb275b800cc]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[26ec828da6d2651f90c74cb275b800cc]
  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\software\microsoft\direct3d[disablemmx]
  Queries value:            HKLM\hardware\devicemap\video[maxobjectnumber]
  Queries value:            HKLM\hardware\devicemap\video[\device\video0]
  Queries value:            HKLM\hardware\devicemap\video[\device\video1]
  Queries value:            HKLM\hardware\devicemap\video[\device\video2]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\bug![name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\bug![flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\bug![id]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[id]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[id]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\msgolf98[name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\msgolf98[flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\msgolf98[id]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[id]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[id]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\rogue squadron[name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\rogue squadron[flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\rogue squadron[id]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\savage[name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\savage[flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\savage[id]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[id]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\silentthunder[name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\silentthunder[flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\silentthunder[id]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\terracide[name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\terracide[flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\terracide[id]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\thirddimension[name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\thirddimension[flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\thirddimension[id]
  Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[name]
  Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[flags]
  Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[id]
  Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[name]
  Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[flags]
  Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[id]
  Queries value:            HKLM\software\microsoft\directdraw[modexonly]
  Queries value:            HKLM\software\microsoft\directdraw[emulationonly]
  Queries value:            HKLM\software\microsoft\directdraw[showframerate]
  Queries value:            HKLM\software\microsoft\directdraw[enableprintscreen]
  Queries value:            HKLM\software\microsoft\directdraw[forceagpsupport]
  Queries value:            HKLM\software\microsoft\directdraw[disableagpsupport]
  Queries value:            HKLM\software\microsoft\directdraw[disablemmx]
  Queries value:            HKLM\software\microsoft\directdraw[disableddscapsinddsd]
  Queries value:            HKLM\software\microsoft\directdraw[disablewidersurfaces]
  Queries value:            HKLM\software\microsoft\directdraw[usenonlocalvidmem]
  Queries value:            HKLM\software\microsoft\directdraw[forcerefreshrate]
  Queries value:            HKLM\software\microsoft\direct3d[flipnovsync]
  Queries value:            HKCU\control panel\desktop[multiuilanguageid]
  Queries value:            HKLM\system\currentcontrolset\control\session
manager\appcompatibility[disableappcompat]
  Queries value:            HKLM\system\wpa\mediacenter[installed]
  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\services\winsock2\parameters[current_protocol_catalog]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[current_namespace_catalog]
  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\direct3d\mostrecentapplication[name]
  Value changes:              HKLM\software\microsoft\directdraw\mostrecentapplication[name]
  Value changes:              HKLM\software\microsoft\directdraw\mostrecentapplication[id]
  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]
```