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: Type: basic admin Owner:

26ec828da6d2651f90c74cb275b800cc Label: Date Added:

2016-05-18 10:30:51 (UTC)

PE32:win32:gui File Type: File Size: 184320 bytes

26ec828da6d2651f90c74cb275b800cc MD5:

2fd94a7ba79df111cbd03365c4ae7ccc17e7dfaba10a30ed3049db2f369c2d4b SHA256:

Description: None

Pattern Matching Results

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
- Opens a recycle bin location
- Creates threads in system processes
- 3 Long sleep detected
- 7 Injects thread into Windows process

Process/Thread Events

C:\WINDOWS\Temp\26ec828da6d2651f90c74cb275b800cc.exe Creates process:

["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

PID:1984 C:\WINDOWS\explorer.exe Writes to process:

Writes to process: PID:896 C:\WINDOWS\system32\services.exe

C:\WINDOWS\Temp\26ec828da6d2651f90c74cb275b800cc.exe Terminates process:

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_ \BaseNamedObjects\DDrawDriverObjectListMutex Creates mutex: Creates mutex: \BaseNamedObjects\MSCTF.Shared.MUTEX.EMH

\BaseNamedObjects\Restricted\{OC5AB9CD-2F90-6754-8374-21D4DAB28CC1} Creates event: Creates event: \BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D78} \BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D77} Creates event:

Creates event:

\BaseNamedObjects\CTF.ThreadMarshalInterfaceEvent.000000E4.00000000.00000004

\BaseNamedObjects\CTF.ThreadMIConnectionEvent.000000E4.00000000.00000004 Creates event:

\BaseNamedObjects\MSCTF.SendReceive.Event.EO.IC Creates event:

Creates event: \BaseNamedObjects\MSCTF.SendReceiveConection.Event.EO.IC \BaseNamedObjects\MSCTF.SendReceive.Event.EMH.IC Creates event:

\BaseNamedObjects\MSCTF.SendReceiveConection.Event.EMH.IC Creates event:

File System Events

Creates: C:\RECYCLER

C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-1003 Creates C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-Creates

1003\\$685c83111e534ea0f6bc8e25bc965f78

Creates C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-

1003\\$685c83111e534ea0f6bc8e25bc965f78\L

C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-Creates:

1003\\$685c83111e534ea0f6bc8e25bc965f78\U

Creates: C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-

1003\\$685c83111e534ea0f6bc8e25bc965f78\@

C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-

1003\\$685c83111e534ea0f6bc8e25bc965f78\n

```
Creates:
                         C:\RECYCLER\
                         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:
 Creates:
                         C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\@
                         C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\n
 Creates:
                         C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-1003\$I5D1DD46B
 Creates:
 Creates:
                         C:GAC MSIL
                         C:\WINDOWS\assembly\GAC
 Creates:
 Creates:
                         C:\WINDOWS\assembly\GAC\Desktop.ini
                         C:\WINDOWS\Prefetch\26EC828DA6D2651F90C74CB275B80-349933DF.pf
 Opens:
 Opens:
                         C:\Documents and Settings\Admin
                         C:\WINDOWS\system32\d3d8.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\d3d8thk.dll
                         C:\WINDOWS\system32\opengl32.dll
 Opens:
 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
                         C:\WINDOWS\Temp\26ec828da6d2651f90c74cb275b800cc.exe
 Opens:
                         C:\WINDOWS\system32\mscat32.dll
 Opens:
 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
                         C:\WINDOWS\AppPatch\systest.sdb
 Opens:
 Opens:
                         C:\WINDOWS\Temp
 Opens:
                         C:\
                         C:\WINDOWS
 Opens:
 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
                         C:\WINDOWS\system32\untfs.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\cabinet.dll
 Opens:
                         C:\WINDOWS\system32\ole32.dll
                         C:\WINDOWS\system32\ws2_32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\ws2help.dll
                         C:\WINDOWS\system32\mswsock.dll
 Opens:
                         {\tt C:\WINDOWS\system32\hnetcfg.dll}
 Opens:
 Opens:
                         C:\WINDOWS\system32\wshtcpip.dll
 Opens:
                         C:\WINDOWS\system32\rsaenh.dll
                         C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-
 Opens:
1003\$685c83111e534ea0f6bc8e25bc965f78
 Opens:
                         C:\Program Files\Windows Defender
 Opens:
                         C:\Program Files\Microsoft Security Client
                         C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-
 Opens:
1003\$685c83111e534ea0f6bc8e25bc965f78\n
                         C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78
 Opens:
 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
                         C:\WINDOWS\assembly\GAC
 Opens:
 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
                         C:\WINDOWS\system32\MSIMTF.dll
 Opens:
                         C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-
1003\$685c83111e534ea0f6bc8e25bc965f78\@
                         C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-
 Writes to:
1003\$685c83111e534ea0f6bc8e25bc965f78\n
                         C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\@
 Writes to:
 Writes to:
                         C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\n
                         C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-1003\$I5D1DD46B
 Writes to:
 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\svstem32\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:	$j.maxmind.com \Rightarrow 127.0.0.1$
Connects to:	127.0.0.1:80
Sends data to:	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 HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: 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 HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: 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 HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: 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 kev: 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 kev: 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: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ gre_initialize$ Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32 Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility HKLM\software\microsoft\windows nt\currentversion\windows Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\winlogon Opens key: HKLM\ $\label{lem:hklm} \verb+ Kklm \+ software \+ microsoft \+ windows nt \+ current version \+ diagnostics$ Opens key: Opens key: HKLM\software\microsoft\direct3d Opens key: HKLM\hardware\devicemap\video HKLM\software\microsoft\directdraw\compatibility Opens key: Opens key: HKLM\software\microsoft\directdraw\compatibility\bug! Opens key: HKLM\software\microsoft\directdraw\compatibility\demolitionderby2 Opens key: $HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus mortal kombat 3$ Opens key: HKLM\software\microsoft\directdraw\compatibility\msgolf98 HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay Opens kev: $HKLM \verb|\software\m| icrosoft \verb|\directdraw\compatibility\nortonsysteminfo$ Opens key: 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: $HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus third dimension$ Opens key: HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark Opens key: $HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus ziff daviswin mark benchmark$ 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 HKCU\control panel\desktop Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msasn1.dll Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$ options\crypt32.dll HKLM\system\currentcontrolset\services\crypt32\performance Opens kev: 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\svstem\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-c000-0000000000046}

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

 $Opens\ key: \\ HKLM\software\microsoft\windows\ nt\currentversion\singe \ file\ execution$

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:

Opens key:

 $HKLM \land system \land current control set \land services \land winsock 2 \land parameters \land protocol_catalog 9 \land catalog_entries 9 \land$

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000001

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000004

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010
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:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace_catalog 5 \setminus 00000004$

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
Opens key:

Opens key:

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: ${\tt HKLM\backslash software\backslash microsoft\backslash windows\ nt\backslash current version\backslash image\ file\ execution}$

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:

9a6f-135d9c6622cc3

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ shells ervice objects \ \ \{f56f6fdd-aa9d-4618$ a949-c1b91af43b1a}

Opens key: HKLM\software\microsoft\windows\currentversion\run

HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key:

options\n

Opens key: HKCU\software\classes\http

HKCR\http Opens key:

Opens key: HKCU\software\classes\http\curver

Opens key: HKCR\http\curver HKCR\http\ Opens key:

Opens key: HKCU\software\classes\http\shell\open

Opens key: HKCR\http\shell\open

HKCU\software\classes\http\shell\open\command Opens kev:

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

HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e} Opens key:

Opens key: HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e} Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-

00805fc1270e}\treatas

Opens key: $HKCR\clsid\balled balled = 5-2166-11d1-b1d0-00805fc1270e$ \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:

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}

HKCR\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e} Opens key:

Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{33c4643c-7811-46fa-a89a-768597bd7223\}$

HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223} Opens kev: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{33c4643c-7811-46fa-a89a-4643c-7811-46fa-a89a-4643c-7811-46fa-a89a-4643c-7811-46fa-a89a-4643c-7811-46fa-a89a-4643c-7811-46fa-a89a-4643c-7811-46fa-a89a-4643c-7811-46fa-a89a-4643c-7811-46fa-a89a-4643c-7811-46fa-a89a-4643c-7811-46fa-a89a-4643c-7811-46fa-a89a-4643c-7811-46fa-a89a-4643c-7811-466a-a89a-4640a-464$ Opens key: 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 kev: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserver32

Opens key:

768597bd7223}\inprocserverx86

Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserverx86

HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-Opens key: 768597bd7223}\localserver32

Opens key:

HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\localserver32

Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-

768597bd7223}\inprochandler32

HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprochandler32 Opens kev:

HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-Opens key:

768597bd7223}\inprochandlerx86

Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprochandlerx86

HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-Opens key:

768597bd7223}\localserver

HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\localserver Opens kev: HKCU\software\policies\microsoft\windows\network connections Opens key: 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

HKCU\software\microsoft\windows\currentversion\explorer\clsid\{2227a280-Opens kev:

3aea-1069-a2de-08002b30309d}

Opens key: HKCU\software\microsoft\windows\currentversion\policies\nonenum Opens key: HKLM\software\microsoft\windows\currentversion\policies\nonenum Opens key:

 $HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ objects \ \ \{2227a280-3aea-1069-1081aea-1069-1081aea-1069-1081aea-1069-1081aea-1081a$

a2de-08002b30309d}

Opens key: $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus explorer \setminus clsid \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus clsid$

```
3aea-1069-a2de-08002b30309d}\shellfolder
                                                                                                           Opens kev:
3aea-1069-a2de-08002b30309d}\shellfolder
                                                                                                            HKCU\software\classes\clsid\{2227a280-3aea-1069-a2de-08002b30309d}
       Opens key:
       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\
                                                                                                            HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-
       Opens key:
00805fc1270e}\shellfolder
                                                                                                            HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\shellfolder
       Opens key:
                                                                                                            HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{7007acc7-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{7007acc7-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{7007acc7-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{7007acc7-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{7007acc7-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{7007acc7-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{7007acc7-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{7007acc7-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{7007acc7-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{7007acc7-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{7007acc7-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{7007acc7-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{7007acc7-microsoft \setminus windows \setminus current version \setminus clsid \setminus explorer \setminus clsid 
       Opens kev:
3202-11d1-aad2-00805fc1270e}
       Opens key:
HKLM \ software \ `microsoft \ `windows \ current version \ shell compatibility \ objects \ \ \{7007acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-11d1-1407acc7-3202-1007acc7-3202-11d1-1407acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-320
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
                                                                                                           HKCU \setminus software \setminus classes \setminus clsid \setminus \{7007acc7-3202-11d1-aad2-00805fc1270e\}
       Opens key:
       Opens key:
                                                                                                            HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}
       Opens key:
                                                                                                            HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\
                                                                                                            Opens kev:
       Opens key:
                                                                                                            HKLM\system\currentcontrolset\services\sharedaccess
       Opens key:
                                                                                                            HKCU\software\classes\applications\calc.exe
       Opens key:
                                                                                                            HKCR\applications\calc.exe
       Opens key:
                                                                                                            Opens key:
                                                                                                            HKLM\software\microsoft\ctf\tip\
                                                                                                           HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
       Opens key:
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}
                                                                                                            HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
       Opens key:
c9633f71be64}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}
                                                                                                            HKLM \ software \ microsoft \ tip \ \{78cb5b0e-26ed-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fc
       Opens key:
77e8f3d1aa80}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}
                                                                                                            HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
      Opens kev:
c9633f71be64}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
                                                                                                            HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
       Opens key:
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
       Opens key:
                                                                                                            HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
c9633f71be64}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
                                                                                                            HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
      Opens kev:
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
                                                                                                            HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
       Opens kev:
c9633f71be64 \\ \\ \\ category \\ \\ \\ item \\ \\ \\ \\ b5a73cd1-8355-426b-a161-259808f26b14 \\ \\ \\ \\
       Opens key:
                                                                                                            HKLM \setminus software \setminus irrosoft \setminus tip \setminus \{78cb5b0e-26ed-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc
77e8f3d1aa80}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}
                                                                                                            HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
      Opens kev:
c9633f71be64}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
                                                                                                            HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
       Opens kev:
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]
       Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
       Queries value:
                                                                                                            HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
                                                                                                            HKLM\software\microsoft\windows
       Oueries value:
nt\currentversion\gre_initialize[disablemetafiles]
                                                                                                            HKLM\software\microsoft\windows
       Queries value:
nt\currentversion\compatibility32[26ec828da6d2651f90c74cb275b800cc]
       Oueries value:
                                                                                                           HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[26ec828da6d2651f90c74cb275b800cc]
                                                                                                            HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
       Oueries value:
       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]
       Oueries value:
                                                                                                            HKLM\hardware\devicemap\video[maxobjectnumber]
       Queries value:
                                                                                                            HKLM\hardware\devicemap\video[\device\video0]
       Queries value:
                                                                                                            HKLM\hardware\devicemap\video[\device\video1]
                                                                                                            HKLM\hardware\devicemap\video[\device\video2]
       Queries value:
                                                                                                            HKLM\software\microsoft\directdraw\compatibility\bug![name]
       Oueries value:
       Oueries value:
                                                                                                            HKLM\software\microsoft\directdraw\compatibility\bug![flags]
                                                                                                            HKLM\software\microsoft\directdraw\compatibility\bug![id]
       Queries value:
       Queries value:
                                                                                                            HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[name]
                                                                                                            HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[flags]
       Oueries value:
                                                                                                            HKLM \verb|\software\m| icrosoft \verb|\directdraw\compatibility\demolitionderby2[id]|
       Queries value:
                                                                                                            HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[name]
       Oueries value:
       Oueries value:
                                                                                                            HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[flags]
       Oueries value:
                                                                                                            HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[id]
       Queries value:
                                                                                                            HKLM\software\microsoft\directdraw\compatibility\msgolf98[name]
       Oueries value:
                                                                                                            HKLM\software\microsoft\directdraw\compatibility\msgolf98[flags]
```

HKLM\software\microsoft\directdraw\compatibility\msgolf98[id]

Queries value:

```
Oueries value:
                                    HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[flags]
  Oueries value:
                                    HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[id]
                                    HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[name]
  Queries value:
                                    HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[flags]
  Oueries value:
  Queries value:
                                    HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[id]
  Oueries value:
                                    HKLM\software\microsoft\directdraw\compatibility\rogue squadron[name]
                                    HKLM\software\microsoft\directdraw\compatibility\rogue squadron[flags]
  Oueries value:
  Oueries value:
                                    HKLM\software\microsoft\directdraw\compatibility\rogue squadron[id]
  Oueries value:
                                    HKLM\software\microsoft\directdraw\compatibility\savage[name]
  Oueries value:
                                    HKLM\software\microsoft\directdraw\compatibility\savage[flags]
  Queries value:
                                    HKLM\software\microsoft\directdraw\compatibility\savage[id]
  Oueries value:
                                    HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[name]
                                    \label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} in the constant \end{tabular} It is a substitution \end{tabular} The constant \end{tabular} in the constant \end{tabular} Th
  Oueries value:
  Queries value:
                                    HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[id]
  Queries value:
                                    HKLM\software\microsoft\directdraw\compatibility\silentthunder[name]
  Oueries 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]
  Oueries 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]
                                    HKLM\software\microsoft\directdraw\compatibility\thirddimension[flags]
  Oueries value:
                                    HKLM\software\microsoft\directdraw\compatibility\thirddimension[id]
  Queries value:
  Queries value:
HKLM \verb|\software\microsoft| direct draw \verb|\compatibility\microsoft| a visual ity benchmark [name] \\
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[flags]
  Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[id]
  Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[name]
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[flags]
  Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[id]
  Oueries value:
                                    HKLM\software\microsoft\directdraw[modexonlv]
  Oueries value:
                                    HKLM\software\microsoft\directdraw[emulationonly]
                                    HKLM\software\microsoft\directdraw[showframerate]
  Queries value:
                                    HKLM\software\microsoft\directdraw[enableprintscreen]
  Queries value:
  Oueries value:
                                    HKLM\software\microsoft\directdraw[forceagpsupport]
                                    {\it HKLM \backslash software \backslash microsoft \backslash direct draw[disable agp support]}
  Queries value:
  Oueries value:
                                    HKLM\software\microsoft\directdraw[disablemmx]
  Oueries value:
                                    HKLM\software\microsoft\directdraw[disableddscapsinddsd]
                                    HKLM\software\microsoft\directdraw[disablewidersurfaces]
  Oueries value:
  Queries value:
                                    HKLM\software\microsoft\directdraw[usenonlocalvidmem]
  Queries value:
                                    HKLM\software\microsoft\directdraw[forcerefreshrate]
  Queries value:
                                    HKLM\software\microsoft\direct3d[flipnovsync]
                                    HKCU\control panel\desktop[multiuilanguageid]
  Oueries value:
  Queries value:
                                    HKLM\system\currentcontrolset\control\session
manager\appcompatibility[disableappcompat]
                                    HKLM\system\wpa\mediacenter[installed]
  Oueries value:
  Queries value:
                                    HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
                                    HKLM\software\microsoft\ole[rwlockresourcetimeout]
  Oueries value:
  Queries value:
                                    HKCR\interface[interfacehelperdisableall]
  Queries value:
                                    HKCR\interface[interfacehelperdisableallforole32]
                                    HKCR\interface[interfacehelperdisabletypelib]
  Oueries value:
  Oueries value:
                                    HKCR\interface\{00020400-0000-0000-c000-
00000000046}[interfacehelperdisableall]
  Queries value:
                                    HKCR\interface\{00020400-0000-0000-c000-
00000000046}[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:
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]
  Oueries 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\00000000003[packedcatalogitem]
```

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ 0000000000005 \ [packed catalog item]$

HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[name]

Oueries value:

Queries value:

Oueries value:

Queries value:

Queries value:

```
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ (000000000007 [packed catalog item]) \ details \ d
                           Oueries value:
```

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000008[packedcatalogitem] Queries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ (000000000009[packed catalog item]) \ details \ de$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem] Oueries 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] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring] Queries value:

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily] Queries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 000000000001[supported name space]$ Queries value:

Queries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace_catalog \ set alog_entries \ (0000000000001[version]) \ details \ det$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000002[librarypath] Queries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000002 \ [displaystring]$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000002[addressfamily] Queries value:

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog 5 \setminus catalog_entries \setminus 0000000000002 [enabled]$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_\catalog_entries\00000000002[storesserviceclassinfo] Queries value:

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] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[addressfamily] Queries value:

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]

Oueries 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]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength] Queries value:

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]

Oueries value:

HKLM\system\currentcontrolset\control\computername\activecomputername[computername]

Oueries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft base

cryptographic provider v1.0[type]

Oueries 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[]
     Oueries value:
                                                                                HKLM\software\clients\startmenuinternet[]
     Queries value:
                                                                                HKLM\software\microsoft\com3[regdbversion]
     Oueries value:
                                                                                HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}[appid]
                                                                                \label{local-equation} \mbox{HKCR} $$ \arrowvert a \arr
     Oueries value:
     Queries value:
                                                                                HKCR\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}[localservice]
     Oueries 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]
     Oueries value:
                                                                                HKCR\clsid\{2227a280-3aea-1069-a2de-
08002b30309d}\shellfolder[wantsfordisplay]
     Queries value:
                                                                                HKCR\clsid\{2227a280-3aea-1069-a2de-
 08002b30309d}\shellfolder[attributes]
                                                                                HKCR\clsid\{2227a280-3aea-1069-a2de-
     Queries value:
 08002b30309d}\shellfolder[callforattributes]
     Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{2227a280-3aea-1069-a2de-
08002b30309d}]
                                                                               HKCR\clsid\{2227a280-3aea-1069-a2de-
     Oueries value:
 08002b30309d}\shellfolder[hidefolderverbs]
                                                                               HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}[localizedstring]
     Queries value:
     Queries value:
HKCU \ software \ microsoft \ windows \ shell no roam \ muicache [@c:\ windows \ system 32 \ shell 32.dll, -9319] \ moreover \ mor
                                                                                HKCR\clsid\{7007acc7-3202-11d1-aad2-
     Queries value:
00805fc1270e}\shellfolder[wantsfordisplay]
                                                                                HKCR\clsid\{7007acc7-3202-11d1-aad2-
 00805fc1270e}\shellfolder[attributes]
     Queries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{7007acc7-3202-11d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2-12d1-aad2
00805fc1270e}1
                                                                                HKCR\clsid\{7007acc7-3202-11d1-aad2-
     Oueries value:
 00805fc1270e}\shellfolder[hidefolderverbs]
                                                                                HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[localizedstring]
     Oueries value:
     Oueries value:
HKCU \ software \ microsoft \ windows \ shell no roam \ muicache [@c: \ windows \ system 32 \ net shell. dll, -1200] \ dll \ dll, -1200] \ dll \ dll
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[current_protocol_catalog]
HKLM\system\currentcontrolset\services\winsock2\parameters[current_namespace_catalog]
     Queries value:
                                                                                HKLM\system\currentcontrolset\services\sharedaccess[start]
HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\calc.exe]
     Queries value:
HKLM \ software \ microsoft \ windows \ current version \ (explorer \ file association \ [cutlist]) \ description \ descriptio
                                                                                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
     Oueries value:
 77e8f3d1aa80}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}[dword]
                                                                                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
     Oueries value:
 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]
                                                                                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
     Oueries value:
 77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[dword]
                                                                                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
     Oueries value:
 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]
                                                                                HKCU\appevents\schemes\apps\.default\systemnotification\.current[]
     Queries value:
     Sets/Creates value:
                                                                                HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-
409d6c4515e9}\inprocserver32[threadingmodel]
                                                                                HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-
     Sets/Creates value:
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]
                                                                                HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32[]
     Value changes:
     Value changes:
 HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 000000000011 [packed catalog item]
     Value changes:
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
```

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ catalog_entries \ 0000000000007 \ [packed catalog item]$

Value changes:

Value changes:

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\00000000004[packedcatalogitem] Value changes:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000003[packedcatalogitem]
 Value changes:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000002[packedcatalogitem] Value changes:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem] Value changes:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Value changes: