Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3329, Task ID: 825

Task ID: 825 Risk Level: 10

Date Processed: 2016-05-18 10:42:23 (UTC)

Processing Time: 62.49 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 Type: PE32:win32:gu 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
- 6 Writes to system32 folder
- 5 Abnormal sleep detected
- Injects thread into Windows process
- 3 Connects to local host
- 6 Changes Winsock providers
- 10 Creates malicious events: ZeroAccess [Rootkit]
- 4 Reads process memory
- 3 Long sleep detected
- 5 Installs service

Process/Thread Events

["C:\windows\temp\26ec828da6d2651f90c74cb275b800cc.exe"]

Creates process: C:\Windows\system32\rundll32.exe [C:\Windows\system32\rundll32.exe

bfe.dll,BfeOnServiceStartTypeChange]

Reads from process: PID:2700 C:\Windows\Temp\26ec828da6d2651f90c74cb275b800cc.exe

Reads from process: PID:2784 C:\Windows\System32\calc.exe

Writes to process: PID:2700 C:\Windows\Temp\26ec828da6d2651f90c74cb275b800cc.exe

Writes to process: PID:1100 C:\Windows\explorer.exe
Writes to process: PID:452 C:\Windows\System32\services.exe

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

Terminates process: C:\Windows\System32\rundl132.exe

Creates remote thread: C:\Windows\explorer.exe

Creates remote thread: C:\Windows\System32\services.exe

Named Object Events

	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	

Creates mutex: \BaseNamedObjects\DBWinMutex

Creates event: \BaseNamedObjects\Restricted\{0C5AB9CD-2F90-6754-8374-21D4DAB28CC1\}
Creates event: \BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D78\}

Creates event: \BaseNamedObjects\SvcctrlStartEvent_A3752DX

Creates event: \BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D77}

File System Events

Creates: C:\\$Recycle.Bin\

Creates: C:\\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-1002

Creates: C:\\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-

1002\\$b136cea6dd8900e373425c26f869789d

Creates: C:\\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-

1002\\$b136cea6dd8900e373425c26f869789d\L

Creates: C:\\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-1002\\$b136cea6dd8900e373425c26f869789d\U

Creates: C:\\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-

1002\\$b136cea6dd8900e373425c26f869789d\@

Creates: C:\\$Recycle.Bin\\$-1-5-21-2160590473-689474908-1361669368-

1002\\$b136cea6dd8900e373425c26f869789d\n

002\\$b136cea6dd8900e373425c26f869789d\n
Creates: C:\Program Files\Windows Defender\en-US:!

Creates: C:\Program Files\Windows Defender\MpAsDesc.dll:!
Creates: C:\Program Files\Windows Defender\MpClient.dll:!
Creates: C:\Program Files\Windows Defender\MpCmdRun.exe:!

Creates: C:\Program Files\Windows Defender\MpCmdRun.exe:!
Creates: C:\Program Files\Windows Defender\MpCommu.dll:!
Creates: C:\Program Files\Windows Defender\MpEvMsg.dll:!

Creates: C:\Program Files\Windows Defender\MpOAV.dll:!

Creates: C:\Program Files\Windows Defender\MpRTP.dll:!

```
C:\Program Files\Windows Defender\MpSvc.dll:!
 Creates:
                         C:\Program Files\Windows Defender\MSASCui.exe:!
 Creates:
 Creates:
                         C:\Program Files\Windows Defender\MsMpCom.dll:!
                         C:\Program Files\Windows Defender\MsMpLics.dll:!
 Creates:
 Creates:
                         C:\Program Files\Windows Defender\MsMpRes.dll:!
 Creates:
                         C:\$Recycle.Bin\S-1-5-18
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d
 Creates:
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\L
 Creates:
 Creates:
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\U
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\@
 Creates:
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\n
 Creates:
 Creates:
                         C:GAC_MSIL
 Creates:
                         C:GAC
                         C:\Windows\assembly\GAC\Desktop.ini
 Creates:
                         C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-1002\$I5D1DD46B
 Creates:
                         C:\Windows\System32\LogFiles\Scm\5c2c622f-70e9-4194-a7da-033e827365ad
 Creates:
 Opens:
                         C:\Windows\Prefetch\26EC828DA6D2651F90C74CB275B80-7FC87F1F.pf
 Opens:
                         C:\Windows\System32
 Opens:
                         C:\windows\temp\D3D8.DLL
 Opens:
                         C:\Windows\System32\d3d8.dll
 Opens:
                         C:\Windows\System32\sechost.dll
 Opens:
                         C:\windows\temp\VERSION.dll
 Opens:
                         C:\Windows\System32\version.dll
 Opens:
                         C:\windows\temp\d3d8thk.dll
 Opens:
                         C:\Windows\System32\d3d8thk.dll
 Opens:
                         C:\windows\temp\dwmapi.dll
 Opens:
                         C:\Windows\System32\dwmapi.dll
 Opens:
                         C:\windows\temp\opengl32.dll
 Opens:
                         C:\Windows\System32\opengl32.dll
 Opens:
                         C:\windows\temp\GLU32.dll
 Opens:
                         C:\Windows\System32\glu32.dll
 Opens:
                         C:\windows\temp\DDRAW.dll
 Opens:
                         C:\Windows\System32\ddraw.dll
 Opens:
                         C:\windows\temp\DCIMAN32.dll
 Opens:
                         C:\Windows\System32\dciman32.dll
 Opens:
                         C:\Windows\System32\imm32.dll
 Opens:
                         C:\Windows\System32\en-US\setupapi.dll.mui
 Opens:
                         C:\windows\temp\MSCAT32.dll
 Opens:
                         C:\Windows\System32\mscat32.dll
 Opens:
                         C:\Windows\Temp\26ec828da6d2651f90c74cb275b800cc.exe
                         C:\Windows\System32\apphelp.dll
 Opens:
 Opens:
                         C:\Windows\System32\ntdll.dll
 Opens:
                         C:\Windows\System32\kernel32.dll
                         C:\Windows\System32\KernelBase.dll
 Opens:
 Opens:
                         C:\Windows\System32\user32.dll
 Opens:
                         C:\Windows\System32\gdi32.dll
 Opens:
                         C:\Windows\System32\lpk.dll
 Opens:
                         C:\Windows\System32\usp10.dll
 Opens:
                         C:\Windows\System32\msvcrt.dll
 Opens:
                         C:\Windows\System32\advapi32.dll
 Opens:
                         C:\Windows\System32\rpcrt4.dll
 Opens:
                         C:\Windows\System32\setupapi.dll
 Opens:
                         C:\Windows\System32\cfgmgr32.dll
 Opens:
                         C:\Windows\System32\oleaut32.dll
 Opens:
                         C:\Windows\System32\ole32.dll
 Opens:
                         C:\Windows\System32\devobj.dll
 Opens:
                         C:\Windows\System32\msctf.dll
 Opens:
                         C:\Windows\System32\wintrust.dll
 Opens:
                         C:\Windows\System32\crypt32.dll
 Opens:
                         C:\Windows\System32\msasn1.dll
 Opens:
                         C:\windows\temp\untfs.dll
                         C:\Windows\System32\untfs.dll
 Opens:
 Opens:
                         C:\windows\temp\Cabinet.dll
 Opens:
                         C:\Windows\System32\cabinet.dll
 Opens:
                         C:\Windows\System32\ws2_32.dll
 Opens:
                         C:\Windows\System32\nsi.dll
 Opens:
                         C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens:
                         C:\Windows\System32\mswsock.dll
 Opens:
                         C:\Windows\System32\WSHTCPIP.DLL
 Opens:
                         C:\windows\temp\CRYPTSP.dll
 Opens:
                         C:\Windows\System32\cryptsp.dll
 Opens:
                         C:\Windows\System32\rsaenh.dll
 Opens:
                         C:\windows\temp\CRYPTBASE.dll
 Opens:
                         C:\Windows\System32\cryptbase.dll
 Opens:
                         C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-
 Opens:
1002\$b136cea6dd8900e373425c26f869789d\n
                         C:\Program Files\Windows Defender
 Opens:
 Opens:
                         C:\Program Files\Windows Defender\en-US
 Opens:
                         C:\Windows\MSWSOCK.dll
 Opens:
                         C:\Program Files\Windows Defender\MpAsDesc.dll
                         C:\Program Files\Windows Defender\MpClient.dll
 Opens:
 Opens:
                         C:\Program Files\Windows Defender\MpCmdRun.exe
```

```
C:\Program Files\Windows Defender\MpCommu.dll
    Opens:
                                                                        C:\Program Files\Windows Defender\MpEvMsg.dll
    Opens:
                                                                        C:\Program Files\Windows Defender\MpOAV.dll
    Opens:
    Opens:
                                                                        C:\Program Files\Windows Defender\MpRTP.dll
    Opens:
                                                                        C:\Program Files\Windows Defender\MpSvc.dll
    Opens:
                                                                        C:\Program Files\Windows Defender\MSASCui.exe
                                                                        C:\Program Files\Windows Defender\MsMpCom.dll
    Opens:
                                                                        C:\Program Files\Windows Defender\MsMpLics.dll
    Opens:
    Opens:
                                                                        C:\Program Files\Windows Defender\MsMpRes.dll
                                                                        C:\Program Files\Microsoft Security Client
    Opens:
    Opens:
                                                                        C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\n
    Opens:
                                                                        C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-1002
    Opens:
                                                                        C:\Windows\assembly
    Opens:
                                                                        C:\Windows\assembly\GAC\Desktop.ini
                                                                        C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\@
    Opens:
                                                                        C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\U
    Opens:
    Opens:
                                                                        C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-
1002\$b136cea6dd8900e373425c26f869789d\@
    Opens:
                                                                        C:\Windows\Temp
                                                                        C:\Windows\System32\rundl132.exe
    Opens:
    Opens:
                                                                        C:\Windows\AppPatch\sysmain.sdb
                                                                        C:\Windows\Prefetch\RUNDLL32.EXE-39102DB5.pf
    Opens:
    Opens:
                                                                        C:\Windows\AppPatch\AcLayers.dll
    Opens:
                                                                        C:\Windows\System32\sspicli.dll
    Opens:
                                                                        C:\Windows\System32\userenv.dll
                                                                        C:\Windows\System32\profapi.dll
    Opens:
    Opens:
                                                                        C:\Windows\System32\winspool.drv
    Opens:
                                                                        C:\Windows\System32\mpr.dll
                                                                        C:\Windows\System32\en-US\rundll32.exe.mui
    Opens:
    Opens:
                                                                        C:\Windows\System32\BFE.DLL
    Opens:
                                                                        C:\Windows\system32\bfe.dll.manifest
    Opens:
                                                                        C:\Windows\system32\bfe.dll.123.Manifest
    Opens:
                                                                        C:\Windows\system32\bfe.dll.124.Manifest
    Opens:
                                                                        C:\Windows\system32\bfe.dll.2.Manifest
    Opens:
                                                                        C:\Windows\System32\authz.dll
    Opens:
                                                                        C:\Windows\System32\slc.dll
    Opens:
                                                                        C:\Windows\System32\LogFiles\Scm\5c2c622f-70e9-4194-a7da-033e827365ad
    Opens:
                                                                        C:\Windows\System32\calc.exe
    Opens:
    Writes to:
                                                                        C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-
1002\$b136cea6dd8900e373425c26f869789d\@
                                                                        C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-
1002\$b136cea6dd8900e373425c26f869789d\n
                                                                        C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\@
   Writes to:
    Writes to:
                                                                        C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\n
    Writes to:
                                                                        C:\Windows\assembly\GAC\Desktop.ini
                                                                        \label{lem:c:secycle.Bin\s-1-5-21-2160590473-689474908-1361669368-1002} \\ \text{C:\shockless} \\ \text{C:\sho
    Writes to:
   Writes to:
                                                                        C:\Windows\System32\LogFiles\Scm\5c2c622f-70e9-4194-a7da-033e827365ad
    Reads from:
                                                                        C:\Windows\Temp\26ec828da6d2651f90c74cb275b800cc.exe
                                                                        \label{lem:c:second} C:\\ensuremath{\tt C:\SRecycle.Bin\S-1-5-18\Sb136cea6dd8900e373425c26f869789d\Sensuremath{\tt C:\SRecycle.Bin\S-1-5-18\Sb136cea6dd8900e373425c26f8696969g\Sensuremath{\tt C:\SRecycle.Bin\S-1-5-18\Sb136cea6dd8900e373425c26f86900e3600000000000000000
    Reads from:
```

Network Events

Reads from:

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

C:\Windows\System32\LogFiles\Scm\5c2c622f-70e9-4194-a7da-033e827365ad

C:\Windows\Temp\26ec828da6d2651f90c74cb275b800cc.exe

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
Sends data to:	86.124.0.99:16471
Sends data to:	68.11.108.202:16471
Pacaiyas data from:	0 0 0 0 0

Receives data from: 0.0.0.0:0

Windows Registry Events

Creates key: HKLM\software\microsoft\direct3d\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

Deletes value: HKLM\software\microsoft\windows\currentversion\run[windows defender]

Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers

Opens key: HKCU\

Opens key: ${\sf HKCU \backslash control\ panel \backslash desktop \backslash muicached \backslash machine language configuration}$

Opens key: HKLM\software\policies\microsoft\mui\settings
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop\languageconfiguration

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
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\

Opens key: HKLM\software\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics

Opens key: HKLM\software\microsoft\direct3d

Opens key: HKLM\software\policies\microsoft\sqmclient\windows

Opens key: ${\tt HKLM \setminus software \setminus microsoft \setminus sqmclient \setminus windows}$

Opens key: HKLM\software\microsoft\ole

Opens key: HKLM\software\microsoft\ole\tracing

Opens key: HKLM\software\microsoft\oleaut

Opens key: HKLM\system\currentcontrolset\control\cmf\config

 $\label{lem:constant} \mbox{ Opens key:} \qquad \mbox{ HKLM\software\microsoft\windows error reporting\wmr} \\ \mbox{ Opens key:} \qquad \mbox{ HKLM\software\microsoft\windows\current\version\setup}$

Opens key: HKLM\software\microsoft\windows\currentversion
Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale

Opens key: HKLM\system\currentcontrolset\services\crypt32

Opens key: HKLM\software\microsoft\windows nt\currentversion\msasn1

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

options\26ec828da6d2651f90c74cb275b800cc.exe

Opens key: HKLM\system\currentcontrol\session manager\appcertdlls
Opens key: HKLM\system\currentcontrol\session manager\appcompatibility

Opens key: HKLM\software\policies\microsoft\windows\appcompat Opens key: HKCU\software\microsoft\windows nt\currentversion Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags HKLM\software\microsoft\windows Opens kev: nt\currentversion\appcompatflags\custom\26ec828da6d2651f90c74cb275b800cc.exe Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernelbase.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: 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\usp10.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: options\lpk.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\gdi32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\user32.dll $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$ Opens kev: options\msctf.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\imm32.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\rpcrt4.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\sechost.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: options\advapi32.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\version.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\dwmapi.dll $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ Opens key: options\d3d8.dll Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$ 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\cfgmgr32.dll Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$ options\ole32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\oleaut32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\devobj.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\setupapi.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\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\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 HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\cabinet.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\nsi.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ws2_32.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: options\dllnxoptions Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\136a17c6 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019

Opens key:

```
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap col_catalog 9 \setminus catalog\_entries
  Opens kev:
```

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001 Opens key:

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:

Opens key:

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:

Opens key:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000011

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000012 Opens key:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ (catalog_entries \ 0000000000013) \ (catalog_entries \ (catalog \ (catalog_entries \ (catalog \ (cata$ Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000014

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000015 Opens key:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ (catalog_entries \ 0000000000016) \ (catalog_entries \ (catalog \ (catalog_entries \ (catalog \ (cata$ Opens key:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ 10000000000017$ Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000018 Opens key:

Opens key:

 $HKLM \ system \ current control set \ services \ win sock 2 \ parameters \ name space_catalog 5 \ 0000000c$ Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001 Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005 Opens key:

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

options\mswsock.dll

Opens key: HKLM\system\currentcontrolset\services\winsock\parameters Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock Opens key: HKLM\system\currentcontrolset\services\psched\parameters\winsock Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers

Opens key:

migration\providers\psched

Opens kev: HKLM\svstem\currentcontrolset\services\tcpip\parameters\winsock

Opens key: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip

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

options\wshtcpip.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\cryptsp.dll

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\system\currentcontrolset\control\lsa\fipsalgorithmpolicy

 ${\tt HKLM \ } system \verb| current control \verb| set \verb| control \verb| lsa$ Opens kev:

Opens key:

HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration HKLM\software\policies\microsoft\cryptography Opens kev:

Opens key: HKLM\software\microsoft\cryptography

Opens key: HKLM\software\microsoft\cryptography\offload

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

options\cryptbase.dll

 $HKLM \backslash software \backslash microsoft \backslash cryptography \backslash deshash session keybackward$ Opens key:

Opens key: HKLM\system\currentcontrolset\services\windefend

Opens key: HKLM\system\currentcontrolset\services\windefend\parameters Opens key: HKLM\system\currentcontrolset\services\windefend\security Opens kev: HKLM\system\currentcontrolset\services\windefend\triggerinfo Opens key: $HKLM \verb|\system| current control set \verb|\services| windefend \verb|\triggerinfo|| 0$

Opens kev:

9a6f-135d9c6622cc}

Opens key:

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

a949-c1b91af43b1a}

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

HKLM\software\microsoft\rpc Opens key:

 $HKLM \verb|\system| current control \verb|\computername| active computername| active computername|$ Opens key:

Opens key: HKLM\system\setup

Opens key: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKLM\system\currentcontrolset\control\sqmservicelist

Opens key: HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32 HKLM\software\microsoft\windows nt\currentversion\profilelist Opens key: Opens key: HKLM\system\currentcontrolset\control\session manager\environment HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-18 Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders

Opens key: HKU\.default\software\microsoft\windows\currentversion\explorer\user

shell folders

Opens key: HKU\.default\environment Opens key: HKU\.default\volatile environment Opens key: HKU\.default\volatile environment\0

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

options\rundll32.exe

Opens key: HKU\.default\software\microsoft\windows

nt\currentversion\appcompatflags\layers

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\rundll32.exe Opens key: HKU\.default\control

panel\desktop\muicached\machinelanguageconfiguration HKU\.default\software\policies\microsoft\control panel\desktop Opens key: Opens key: HKU\.default\control panel\desktop\languageconfiguration

Opens key: HKU\.default\control panel\desktop

Opens key: HKU\.default\control panel\desktop\muicached

Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags Opens key: HKU\.default\software\microsoft\windows nt\currentversion\appcompatflags

 ${\tt HKLM \ } system \verb|\ current control \ set \verb|\ control \ | network provider \verb|\ hworder| \\$ Opens key:

Opens key: HKLM\system\currentcontrolset\services\bfe

Opens key: HKLM\system\currentcontrolset\services\aelookupsvc

HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo Opens key: Opens key: Opens key: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\1

HKLM\system\currentcontrolset\services\alg Opens key: Opens key: HKLM\system\currentcontrolset\services\alg\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\appidsvc

Opens key:

Opens key: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0 Opens kev: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\1

 ${\it HKLM} \verb|\system| current control set \verb|\services| appinfo$ Opens key:

Opens key: HKLM\system\currentcontrolset\services\appinfo\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\appmgmt

Opens key: HKLM\system\currentcontrolset\services\appmgmt\triggerinfo Opens key: HKLM\system\currentcontrolset\services\audioendpointbuilder

Opens key: HKLM\system\currentcontrolset\services\audioendpointbuilder\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\audiosrv

Opens key: HKLM\system\currentcontrolset\services\audiosrv\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\axinstsv

Opens key: HKLM\system\currentcontrolset\services\axinstsv\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\bdesvc

Opens key: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo $HKLM \verb|\system| current controlset \verb|\services| bdesvc \verb|\triggerinfo|| 0$ Opens key: Opens key: HKLM\system\currentcontrolset\services\bfe\triggerinfo Opens key:

 ${\it HKLM \ } system \verb| current control set \verb| services \verb| bits \\$ Opens key:

Opens key: HKLM\system\currentcontrolset\services\bits\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\browser

 ${\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ browser \verb|\ triggerinfo|$ Opens key: Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo\0 Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo\1 $HKLM \verb|\system| current control set \verb|\services| browser \verb|\triggerinfo|| 2$ Opens key:

Opens key: HKLM\system\currentcontrolset\services\bthserv

Opens key: HKLM\svstem\currentcontrolset\services\bthserv\triggerinfo $\label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ services \+ bthserv \+ trigger in fo \+ 0$ Opens key: Opens key:

Opens kev: HKLM\svstem\currentcontrolset\services\certpropsvc

Opens key: HKLM\system\currentcontrolset\services\certpropsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32

Opens key:

HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\comsysapp

Opens key: HKLM\system\currentcontrolset\services\comsysapp\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\cryptsvc
Opens key: HKLM\system\currentcontrolset\services\cryptsvc\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\cscservice

Opens key: HKLM\system\currentcontrolset\services\cscservice\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\dcomlaunch

Opens key: HKLM\system\currentcontrolset\services\dcomlaunch\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\defragsvc

Opens key: ${\tt HKLM \backslash system \backslash current control set \backslash services \backslash defrags vc \backslash trigger info}$

Opens key: HKLM\system\currentcontrolset\services\dhcp

Opens key: HKLM\system\currentcontrolset\services\dhcp\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\dnscache

Opens key: HKLM\system\currentcontrolset\services\dnscache\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\1

Opens key: HKLM\system\currentcontrolset\services\dot3svc

Opens key: HKLM\system\currentcontrolset\services\dot3svc\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\dps

Opens key: HKLM\system\currentcontrolset\services\dps\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\eaphost

Opens key: HKLM\system\currentcontrolset\services\eaphost\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\efs

Opens key: HKLM\system\currentcontrolset\services\efs\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\efs\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\efs\triggerinfo\1

Opens key: HKLM\system\currentcontrolset\services\ehrecvr

Opens key: HKLM\system\currentcontrolset\services\ehrecvr\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\ehsched

Opens key: HKLM\system\currentcontrolset\services\ehsched\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\eventlog

Opens key: HKLM\system\currentcontrolset\services\eventlog\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\eventsystem

Opens key: HKLM\system\currentcontrolset\services\eventsystem\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\fax

Opens key: HKLM\system\currentcontrolset\services\fax\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\fdphost
Opens key: HKLM\system\currentcontrolset\services\fdphost\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\fdrespub

Opens key: HKLM\system\currentcontrolset\services\fdrespub\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\fontcache

Opens key: HKLM\system\currentcontrolset\services\fontcache\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\fontcache3.0.0.0

Opens key: HKLM\system\currentcontrolset\services\fontcache3.0.0.0\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\gpsvc

Opens key: HKLM\system\currentcontrolset\services\gpsvc\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\hidserv

Opens key: HKLM\system\currentcontrolset\services\hidserv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\1

Opens key: HKLM\system\currentcontrolset\services\hkmsvc

Opens key: HKLM\system\currentcontrolset\services\hkmsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\homegrouplistener

Opens key: HKLM\system\currentcontrolset\services\homegrouplistener\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\homegroupprovider

Opens key: HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\idsvc
Opens key: HKLM\system\currentcontrolset\services\idsvc\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\ikeext
Opens key: HKLM\system\currentcontrolset\services\ikeext\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\1

Opens key: HKLM\system\currentcontrolset\services\ipbusenum

Opens key: HKLM\system\currentcontrolset\services\ipbusenum\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\ivmservice Opens key: HKLM\system\currentcontrolset\services\keyiso

Opens key: ${\tt HKLM \ } {\tt LKLM \ } {\tt LK$

Opens key: HKLM\system\currentcontrolset\services\ktmrm

Opens key: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\lanmanserver

Opens key: HKLM\system\currentcontrolset\services\lanmanserver\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\lanmanworkstation

 $Opens\ key: \\ HKLM \ system \ current control set \ services \ lanman work station \ trigger in formal station \ trigger in formal services \ land \ description \ descr$

Opens key: HKLM\system\currentcontrolset\services\lltdsvc

Opens key: HKLM\system\currentcontrolset\services\lltdsvc\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\lmhosts

Opens key: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo Opens key: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0

HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1 Opens key: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2 Opens key: HKLM\system\currentcontrolset\services\mcx2svc Opens kev: Opens key: HKLM\system\currentcontrolset\services\mcx2svc\triggerinfo Opens kev: HKLM\system\currentcontrolset\services\mmcss Opens key: HKLM\system\currentcontrolset\services\mmcss\triggerinfo HKLM\system\currentcontrolset\services\msdtc Opens key: HKLM\system\currentcontrolset\services\msdtc\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\msiscsi HKLM\system\currentcontrolset\services\msiscsi\triggerinfo Opens key: Opens key: HKLM\svstem\currentcontrolset\services\msiserver Opens key: HKLM\system\currentcontrolset\services\msiserver\triggerinfo Opens key: HKLM\system\currentcontrolset\services\napagent HKLM\system\currentcontrolset\services\napagent\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\netlogon HKLM\system\currentcontrolset\services\netlogon\triggerinfo Opens key: Opens key: HKLM\software\microsoft\sqmclient\windows\disabledprocesses\ Opens key: HKLM\software\microsoft\sqmclient\windows\disabledsessions\ Opens key: HKLM\system\currentcontrolset\services\netman Opens key: HKLM\system\currentcontrolset\services\netman\triggerinfo Opens key: HKLM\system\currentcontrolset\services\netprofm HKLM\system\currentcontrolset\services\netprofm\triggerinfo Opens key: HKLM\system\currentcontrolset\services\nettcpportsharing Opens kev: Opens key: HKLM\system\currentcontrolset\services\nettcpportsharing\triggerinfo Opens key: HKLM\system\currentcontrolset\services\nlasvc Opens key: HKLM\system\currentcontrolset\services\nlasvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\nsi Opens key: HKLM\system\currentcontrolset\services\nsi\triggerinfo HKLM\system\currentcontrolset\services\ose Opens kev: Opens key: HKLM\system\currentcontrolset\services\ose\triggerinfo Opens key: HKLM\system\currentcontrolset\services\p2pimsvc Opens key: HKLM\system\currentcontrolset\services\p2pimsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\p2psvc Opens key: HKLM\system\currentcontrolset\services\p2psvc\triggerinfo HKLM\system\currentcontrolset\services\pcasvc Opens key: Opens key: HKLM\system\currentcontrolset\services\pcasvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\peerdistsvc HKLM\system\currentcontrolset\services\peerdistsvc\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\pla Opens key: HKLM\system\currentcontrolset\services\pla\triggerinfo HKLM\system\currentcontrolset\services\plugplay Opens key: Opens key: HKLM\system\currentcontrolset\services\plugplay\triggerinfo Opens key: HKLM\system\currentcontrolset\services\pnrpautoreg HKLM\system\currentcontrolset\services\pnrpautoreg\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\pnrpsvc Opens key: HKLM\system\currentcontrolset\services\pnrpsvc\triggerinfo HKLM\system\currentcontrolset\services\policyagent Opens key: Opens key: HKLM\system\currentcontrolset\services\policyagent\triggerinfo Opens key: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0 $HKLM \verb|\system| current controlset \verb|\services| policy agent \verb|\triggerinfo| 1$ Opens key: Opens key: HKLM\system\currentcontrolset\services\power Opens key: HKLM\system\currentcontrolset\services\power\triggerinfo Opens key: HKLM\system\currentcontrolset\services\profsvc Opens key: HKLM\system\currentcontrolset\services\profsvc\triggerinfo Opens kev: HKLM\system\currentcontrolset\services\protectedstorage Opens key: HKLM\system\currentcontrolset\services\protectedstorage\triggerinfo Opens key: HKLM\system\currentcontrolset\services\qwave Opens key: HKLM\system\currentcontrolset\services\qwave\triggerinfo HKLM\system\currentcontrolset\services\rasauto Opens key: Opens key: HKLM\system\currentcontrolset\services\rasauto\triggerinfo Opens key: HKLM\system\currentcontrolset\services\rasman Opens key: HKLM\system\currentcontrolset\services\rasman\triggerinfo Opens key: HKLM\system\currentcontrolset\services\remoteaccess Opens key: HKLM\system\currentcontrolset\services\remoteaccess\triggerinfo HKLM\system\currentcontrolset\services\remoteregistry Opens key: Opens key: HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo Opens key: HKLM\system\currentcontrolset\services\rpceptmapper Opens key: ${\tt HKLM \ } system \verb|\ current controlset \ \verb|\ services \ \verb|\ rpceptmapper \ \verb|\ triggerinfo|$ Opens key: HKLM\system\currentcontrolset\services\rpclocator Opens key: HKLM\system\currentcontrolset\services\rpclocator\triggerinfo

Opens key: ${\tt HKLM \setminus system \setminus current control set \setminus services \setminus rpcss}$

Opens key: HKLM\system\currentcontrolset\services\rpcss\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\samss
Opens key: HKLM\system\currentcontrolset\services\samss\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\scardsvr\triggerinfo

HKLM\system\currentcontrolset\services\scardsvr\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\schedule

Opens key: HKLM\system\currentcontrolset\services\schedule\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\scpolicysvc

Opens key: HKLM\system\currentcontrolset\services\scpolicysvc\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\sdrsvc

Opens key: HKLM\system\currentcontrolset\services\sdrsvc\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\seclogon

HKLM\system\currentcontrolset\services\seclogon\triggerinfo Opens key: HKLM\system\currentcontrolset\services\sens Opens key: Opens kev: HKLM\system\currentcontrolset\services\sens\triggerinfo Opens key: HKLM\system\currentcontrolset\services\sensrsvc Opens kev: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1 Opens key: Opens key: HKLM\system\currentcontrolset\services\sessionenv HKLM\system\currentcontrolset\services\sessionenv\triggerinfo Opens key: HKLM\system\currentcontrolset\services\shellhwdetection Opens key: Opens key: HKLM\system\currentcontrolset\services\shellhwdetection\triggerinfo Opens key: HKLM\system\currentcontrolset\services\snmptrap Opens key: HKLM\system\currentcontrolset\services\snmptrap\triggerinfo HKLM\system\currentcontrolset\services\spooler Opens key: HKLM\system\currentcontrolset\services\spooler\triggerinfo Opens key: HKLM\system\currentcontrolset\services\sppsvc Opens key: HKLM\system\currentcontrolset\services\sppsvc\triggerinfo Opens kev: Opens key: HKLM\system\currentcontrolset\services\sppuinotify Opens key: HKLM\system\currentcontrolset\services\sppuinotify\triggerinfo Opens key: HKLM\system\currentcontrolset\services\ssdpsrv HKLM\system\currentcontrolset\services\ssdpsrv\triggerinfo Opens key: HKLM\system\currentcontrolset\services\sstpsvc Opens key: HKLM\system\currentcontrolset\services\sstpsvc\triggerinfo Opens kev: Opens key: HKLM\system\currentcontrolset\services\stisvc Opens key: HKLM\system\currentcontrolset\services\stisvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\storsvc Opens key: HKLM\system\currentcontrolset\services\storsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0 HKLM\system\currentcontrolset\services\storsvc\triggerinfo\1 Opens kev: Opens key: HKLM\system\currentcontrolset\services\swprv Opens key: HKLM\system\currentcontrolset\services\swprv\triggerinfo Opens key: HKLM\system\currentcontrolset\services\sysmain Opens key: HKLM\system\currentcontrolset\services\sysmain\triggerinfo Opens key: HKLM\system\currentcontrolset\services\tabletinputservice Opens key: HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\1 HKLM\system\currentcontrolset\services\tapisrv Opens key: Opens key: HKLM\system\currentcontrolset\services\tapisrv\triggerinfo Opens key: HKLM\system\currentcontrolset\services\tbs HKLM\system\currentcontrolset\services\tbs\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\termservice Opens key: HKLM\system\currentcontrolset\services\termservice\triggerinfo HKLM\system\currentcontrolset\services\themes Opens key: Opens key: HKLM\system\currentcontrolset\services\themes\triggerinfo Opens key: HKLM\system\currentcontrolset\services\threadorder Opens key: ${\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ thread order \verb|\ trigger info$ Opens key: ${\it HKLM \ } system \ `current control set \ `services \ `tlntsvr"$ HKLM\system\currentcontrolset\services\tlntsvr\triggerinfo Opens kev: Opens key: HKLM\system\currentcontrolset\services\trkwks Opens key: HKLM\system\currentcontrolset\services\trkwks\triggerinfo Opens key: HKLM\system\currentcontrolset\services\trustedinstaller Opens key: HKLM\system\currentcontrolset\services\trustedinstaller\triggerinfo Opens key: HKLM\system\currentcontrolset\services\ui0detect Opens kev: HKLM\system\currentcontrolset\services\ui0detect\triggerinfo Opens key: HKLM\system\currentcontrolset\services\umrdpservice Opens key: HKLM\system\currentcontrolset\services\umrdpservice\triggerinfo Opens key: HKLM\system\currentcontrolset\services\upnphost HKLM\system\currentcontrolset\services\upnphost\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\uxsms Opens key: HKLM\system\currentcontrolset\services\uxsms\triggerinfo HKLM\system\currentcontrolset\services\vaultsvc Opens key: Opens key: HKLM\system\currentcontrolset\services\vaultsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\vds HKLM\system\currentcontrolset\services\vds\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\vss Opens key: HKLM\system\currentcontrolset\services\vss\triggerinfo Opens key: HKLM\system\currentcontrolset\services\w32time Opens key: HKLM\system\currentcontrolset\services\w32time\triggerinfo Opens key: HKLM\system\currentcontrolset\services\w32time\triggerinfo\0 $HKLM \verb| system| current control set \verb| services| \verb| w32time| trigger in fo| 1$ Opens key: Opens key: HKLM\system\currentcontrolset\services\w32time\triggerinfo\2 Opens key: HKLM\system\currentcontrolset\services\wbengine ${\it HKLM} \verb|\system| current controlset| services| when gine \verb|\triggerinfo| \\$ Opens key: Opens key: HKLM\system\currentcontrolset\services\wbiosrvc HKLM\system\currentcontrolset\services\wbiosrvc\triggerinfo Opens kev:

 ${\it HKLM} \verb|\system| current control set \verb|\services| wcncsvc$ Opens key: Opens key: HKLM\system\currentcontrolset\services\wcncsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\wcspluginservice Opens key:

HKLM\system\currentcontrolset\services\wcspluginservice\triggerinfo

Opens key: ${\it HKLM \ } system \ `current control set \ `services \ `wdiservice host" \\$

HKLM\system\currentcontrolset\services\wdiservicehost\triggerinfo Opens kev:

Opens key: HKLM\system\currentcontrolset\services\wdisystemhost

```
HKLM\system\currentcontrolset\services\wdisystemhost\triggerinfo
  Opens key:
  Opens key:
                                   HKLM\system\currentcontrolset\services\webclient
  Opens kev:
                                   HKLM\system\currentcontrolset\services\webclient\triggerinfo
  Opens key:
                                   HKLM\system\currentcontrolset\services\webclient\triggerinfo\0
  Opens kev:
                                   HKLM\system\currentcontrolset\services\webclient\triggerinfo\1
  Opens key:
                                   HKLM\system\currentcontrolset\services\wecsvc
                                   HKLM\system\currentcontrolset\services\wecsvc\triggerinfo
  Opens key:
  Opens key:
                                   HKLM\system\currentcontrolset\services\wercplsupport
                                   HKLM\system\currentcontrolset\services\wercplsupport\triggerinfo
  Opens key:
                                   HKLM\system\currentcontrolset\services\wersvc
  Opens key:
  Opens key:
                                   HKLM\system\currentcontrolset\services\wersvc\triggerinfo
  Opens key:
                                   Opens key:
                                   HKLM\system\currentcontrolset\services\wersvc\triggerinfo\1
                                   HKLM\system\currentcontrolset\services\winhttpautoproxysvc
  Opens key:
  Opens key:
                                   HKLM\system\currentcontrolset\services\winhttpautoproxysvc\triggerinfo
                                   HKLM\system\currentcontrolset\services\winmgmt
  Opens key:
                                   HKLM\system\currentcontrolset\services\winmgmt\triggerinfo
  Opens kev:
  Opens key:
                                   HKLM\system\currentcontrolset\services\winrm
  Opens key:
                                   HKLM\system\currentcontrolset\services\winrm\triggerinfo
                                   HKLM\system\currentcontrolset\services\wlansvc
  Opens key:
  Opens key:
                                   HKLM\system\currentcontrolset\services\wlansvc\triggerinfo
  Opens key:
                                   HKLM\system\currentcontrolset\services\wmiapsrv
                                   HKLM\system\currentcontrolset\services\wmiapsrv\triggerinfo
  Opens kev:
  Opens key:
                                   HKLM\system\currentcontrolset\services\wmpnetworksvc
  Opens key:
                                   HKLM\system\currentcontrolset\services\wmpnetworksvc\triggerinfo
  Opens key:
                                   HKLM\system\currentcontrolset\services\wpcsvc
  Opens key:
                                   HKLM\system\currentcontrolset\services\wpcsvc\triggerinfo
  Opens key:
                                   HKLM\system\currentcontrolset\services\wpdbusenum
  Opens key:
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo
  Opens key:
                                   HKLM \verb|\system| current controlset \verb|\services| wpdbusenum \verb|\triggerinfo|| 0
  Opens key:
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2
  Opens key:
  Opens key:
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3
  Opens key:
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4
                                   HKLM\system\currentcontrolset\services\wsearch
  Opens key:
  Opens key:
                                   HKLM\system\currentcontrolset\services\wsearch\triggerinfo
  Opens key:
                                   HKLM\system\currentcontrolset\services\wuauserv
                                   HKLM\system\currentcontrolset\services\wuauserv\triggerinfo
  Opens key:
  Opens key:
                                   HKLM\system\currentcontrolset\services\wudfsvc
  Opens key:
                                   HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo
                                   HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0
  Opens key:
  Opens key:
                                   Opens key:
                                   HKLM\system\currentcontrolset\services\wwansvc
                                   HKLM\system\currentcontrolset\services\wwansvc\triggerinfo
  Opens key:
  Opens key:
                                   HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
  Opens key:
                                   HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
                                   HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
  Opens key:
355b7f55341b}\treatas
                                   HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\treatas
  Opens kev:
                                   HKCU \setminus software \setminus classes \setminus clsid \setminus \{660b90c8-73a9-4b58-8cae-18b60b90c8-73a9-4b58-8cae-18b60b90c8-73a9-4b58-8cae-18b60b90c8-73a9-4b58-8cae-18b60b90c8-73a9-4b58-8cae-18b60b90c8-73a9-4b58-8cae-18b60b90c8-73a9-4b58-8cae-18b60b90c8-73a9-4b58-8cae-18b60b90c8-73a9-4b58-8cae-18b60b90c8-73a9-4b58-8cae-18b60b90c8-73a9-4b58-8cae-18b60b90c8-73a9-4b58-8cae-18b60b90c8-73a9-4b58-8cae-18b60b90c8-73a9-4b58-8cae-18b60b90c8-73a9-4b58-8cae-18b60b90c8-73a9-4b58-8cae-18b60b90c8-73a9-4b58-8cae-18b60b90c8-73a9-4b58-8cae-18b60b90c8-73a9-4b58-8cae-18b60b90c8-73a9-4b58-8cae-18b60b90c8-73a9-8cae-18b60b90c8-73a9-8cae-18b60b90c8-73a9-8cae-18b60b90c8-73a9-8cae-18b60b90c8-73a9-8cae-18b60b90c8-73a9-8cae-18b60b90c8-73a9-8cae-18b60b90c8-73a9-8cae-18b60b90c8-73a9-8cae-18b60b90c8-73a9-8cae-18b60b90c8-73a9-8cae-18b60b90c8-73a9-8cae-18b60b90c8-73a9-8cae-18b60b90c8-73a9-8cae-18b60b90c8-73a9-8cae-18b60b90c8-73a9-8cae-18b60b90c8-73a9-8cae-18b60b90c8-73a9-8cae-18b60b90c8-73a9-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c8-75a0-8cae-18b60b90c9-8cae-18b60b90c9-8cae-18b60b90c9-8cae-18b60b90c9-8cae-18b60b90c9-8cae-18b60b90c9-8cae-18b60b90c9-8cae-18b60b90c9-8cae-18b60b90c9-8cae-18b60b90c9-8cae-18b60b90c9-8cae-18b60b90c9-8cae-18b60b90c9-8cae-
  Opens key:
355b7f55341b}\progid
                                   HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\progid
  Opens key:
                                   HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
  Opens key:
355b7f55341b}\inprocserver32
  Opens kev:
                                   HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32
  Opens key:
                                   HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\inprochandler32
                                   HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler32
  Opens key:
                                   HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
  Opens key:
355b7f55341b}\inprochandler
  Opens key:
                                   HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler
                                   \label{local-eq:hkcu} \begin{tabular}{ll} HKCU \software \classes \clsid \alpha 2a9545d-a0c2-42b4-9708-a0b2badd77c8} \end{tabular}
  Opens key:
  Opens key:
                                   HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}
  Opens key:
                                   HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\treatas
  Opens key:
                                   HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\treatas
  Opens key:
                                   HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\progid
  Opens key:
                                   HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\progid
  Opens key:
                                   HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprocserver32
  Opens key:
                                   HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprocserver32
  Opens key:
                                   HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprochandler32
  Opens key:
                                   HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprochandler32
                                   HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-
  Opens kev:
a0b2badd77c8}\inprochandler
  Opens key:
                                   HKCR \clsid \a2a9545d-a0c2-42b4-9708-a0b2badd77c8 \hiprochandler
  Opens key:
                                   HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}
                                   HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}
  Opens key:
  Opens key:
                                   HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-
535773d48449}\treatas
```

Opens key: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\treatas

Opens key: HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-

535773d48449}\progid

535773d48449}\inprocserver32

Opens key: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprocserver32

Opens key: HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-

535773d48449}\inprochandler32

Opens key: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprochandler32

Opens key: HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-

535773d48449}\inprochandler

Opens key: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprochandler

Opens key: HKCU\software\classes\applications\calc.exe

Opens key: HKCR\applications\calc.exe

Opens key: HKLM\software\microsoft\ctf\knownclasses

Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}

Opens key: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}
Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-

0000f87a470c}\treatas

 $\label{lem:continuous} Opens~key: $$ HKCR\clsid\dd313e04-feff-11d1-8ecd-0000f87a470c\treatas $$ Opens~key: $$ HKCU\software\classes\clsid\dd313e04-feff-11d1-8ecd-$$$

0000f87a470c}\progid

Opens key: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\progid Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-

0000f87a470c}\inprocserver32

Opens key: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32

Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-

0000f87a470c}\inprochandler32

Opens key: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprochandler32

Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-

0000f87a470c}\inprochandler

Opens key: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprochandler

Queries value: HKLM\system\currentcontrolset\control\session

manager[cwdillegalindllsearch]

Queries value: HKLM\system\currentcontrol\set\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrol\set\control\terminal server[tsuserenabled]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]

Queries value: HKCU\control panel\desktop[preferreduilanguages]

Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]

Queries value:

HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKLM\system\currentcontrol\set\control\nls\sorting\versions[]

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\windows[loadappinit_dlls]

Queries value: HKLM\software\microsoft\direct3d[disablemmx]

 Queries value:
 HKLM\software\microsoft\sqmclient\windows[ceipenable]

 Queries value:
 HKLM\software\microsoft\ole[pageallocatorusesystemheap]

 Queries value:
 HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]

 Queries value:
 HKLM\system\currentcontrolset\config[system]

Queries value: HKLM\software\microsoft\windows\error reporting\mmr[disable]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
Queries value: HKLM\software\microsoft\windows\currentversion[devicepath]
Queries value: HKLM\system\currentcontrol\set\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrol\set\control\nls\extendedlocale[en-us]
Queries value: HKLM\system\currentcontrol\set\services\crypt32[debugheapflags]

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options[disablelocaloverride]

 $\label{thm:linear} Queries \ value: \\ HKLM \ software \ microsoft \ windows \ nt \ current version \ image \ file \ execution \\$

options\dllnxoptions[usefilter]

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\dllnxoptions[untfs.dll]

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap services \setminus winsock _registry_version]$

Queries value:

Queries value:

 $\label{lem:hklm} $\tt HKLM \setminus System \setminus current control set \setminus services \setminus winsock 2 \cap col_catalog 9 [serial_access_num] \\$

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]

Queries value:

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\0000000000002[packedcatalogitem]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000003[packedcatalogitem]

Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem] Oueries 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries \ 000000000017 \ [packed catalog item] \\ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Oueries 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\00000000001[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
 Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 00000000000002 \ [version] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerid]
 Oueries 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] Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \names pace_catalog 5 \catalog_entries \names \pace_catalog 5 \catalog_entries \pace_catalog 5 \catalog 6 \catalog 6 \catalog 6 \catalog 6 \catalog 6 \c$

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
 Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 0000000000004 [storesservice class info] \\ Oueries \ value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerid]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[enabled]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[version] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[storesserviceclassinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerinfo]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[providerid]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[enabled] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[providerinfo]

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

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws 2_32 spin count]$

Oueries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]

Queries value:

HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\psched[winsock 2.0 provider id]

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

Queries value: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip[winsock 2.0 provider id]

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

 $\label{thm:local_queries} Queries \ value: \\ HKLM \ software \ microsoft \ cryptography \ defaults \ provider \ microsoft \ base \\$

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\system\currentcontrol\sa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrol\sa[fipsalgorithmpolicy]
Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]

Oueries value:

HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]

Queries value: HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]

Queries value: HKLM\software\microsoft\cryptography[machineguid]

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\dllnxoptions[n]

Queries value: HKLM\software\microsoft\rpc[maxrpcsize]

Queries value:

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

Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup[systemsetupinprogress]

Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]

Oueries value:

 $\label{lem:hklm} \verb+Kklm/system/currentcontrolset/services/winsock2\parameters[current_protocol_catalog]+ \parameters[current_protocol_catalog]+ \parameters[current_protocol_catalog]+ \parameters[current_protocol$

Queries value:

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

Queries value: HKLM\software\microsoft\windows

nt\currentversion\profilelist[programdata]

HKLM\software\microsoft\windows nt\currentversion\profilelist[public] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[default] Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir] Oueries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir] Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir (x86)] Queries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir (x86)] Oueries value: HKLM\software\microsoft\windows\currentversion[programw6432dir] Queries value: HKLM\software\microsoft\windows\currentversion[commonw6432dir] Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-

18[profileimagepath]

Queries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user

shell folders[appdata]

Queries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user

shell folders[local appdata]

Queries value: HKU\.default\control panel\desktop[preferreduilanguages]

Queries value: HKU\.default\control
panel\desktop\muicached[machinepreferreduilanguages]
Queries value: HKLM\software\microsoft\windows

nt\currentversion\compatibility32[rundll32]

 Queries value:
 HKLM\system\currentcontrolset\services\bfe[imagepath]

 Queries value:
 HKLM\system\currentcontrolset\services\bfe[type]

 Queries value:
 HKLM\system\currentcontrolset\services\bfe[start]

 Queries value:
 HKLM\system\currentcontrolset\services\bfe[errorcontrol]

Queries value: HKLM\system\currentcontrolset\services\bfe[tag]

 Queries value:
 HKLM\system\currentcontrolset\services\bfe[dependonservice]

 Queries value:
 HKLM\system\currentcontrolset\services\bfe[dependongroup]

 Queries value:
 HKLM\system\currentcontrolset\services\bfe[group]

 Queries value:
 HKLM\system\currentcontrolset\services\bfe[objectname]

Queries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[guid]

Queries value:

Queries value:

Oueries value:

Queries value:

HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[datatype0]

HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[action] Oueries value: Queries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[type] Queries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[guid] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus appids vc \setminus trigger info \setminus 0 \ [data type 0]$ HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[action] Queries value: Queries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[type] Oueries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[guid] Queries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[datatype0] Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[action] Oueries value: Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[guid] Queries value: HKLM\svstem\currentcontrolset\services\browser\triggerinfo\0ſdatatype01 Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data0] HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype1] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data1] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype2] Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data2] Queries value: HKLM\svstem\currentcontrolset\services\browser\triggerinfo\0ſdatatype31 Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[action] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[type] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[guid] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype0]

HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data0]

HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data1]

HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype1]

```
HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data2]
 Oueries value:
 Oueries value:
                         HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype3]
 Queries value:
                         HKLM\system\currentcontrolset\services\browser[imagepath]
 Oueries value:
                         HKLM\system\currentcontrolset\services\browser[type]
 Queries value:
                         HKLM\system\currentcontrolset\services\browser[start]
 Oueries value:
                         HKLM\system\currentcontrolset\services\browser[errorcontrol]
                         HKLM\svstem\currentcontrolset\services\browser[tag]
 Oueries value:
 Oueries value:
                         HKLM\system\currentcontrolset\services\browser[dependonservice]
 Oueries value:
                         HKLM\system\currentcontrolset\services\browser[dependongroup]
 Oueries value:
                         HKLM\system\currentcontrolset\services\browser[group]
 Queries value:
                         HKLM\system\currentcontrolset\services\browser[objectname]
 Oueries value:
                         HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[action]
                         HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[type]
 Oueries value:
 Oueries value:
                         HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[guid]
 Oueries value:
                         HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[datatype0]
 Queries value:
                         HKLM\svstem\currentcontrolset\services\dnscache\triggerinfo\0[action]
 Queries value:
                         HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[type]
 Oueries value:
                         HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[guid]
 Oueries value:
                         HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[datatype0]
 Queries value:
                         HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[data0]
 Queries value:
                         HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[datatype1]
 Queries value:
                         HKLM\system\currentcontrolset\services\dnscache[imagepath]
 Queries value:
                         HKLM\system\currentcontrolset\services\dnscache[type]
 Oueries value:
                         HKLM\system\currentcontrolset\services\dnscache[start]
 Oueries value:
                         HKLM\system\currentcontrolset\services\dnscache[errorcontrol]
 Queries value:
                         HKLM\system\currentcontrolset\services\dnscache[tag]
 Queries value:
                         HKLM\system\currentcontrolset\services\dnscache[dependonservice]
 Oueries value:
                         HKLM\system\currentcontrolset\services\dnscache[dependongroup]
 Queries value:
                         HKLM\system\currentcontrolset\services\dnscache[group]
 Queries value:
                         HKLM\svstem\currentcontrolset\services\dnscache[objectname]
 Oueries value:
                         HKLM\system\currentcontrolset\services\efs\triggerinfo\0[action]
                         HKLM\system\currentcontrolset\services\efs\triggerinfo\0[type]
 Queries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\efs\triggerinfo\0[guid]
 Oueries value:
                         HKLM\system\currentcontrolset\services\efs\triggerinfo\0[datatype0]
                         HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[action]
 Queries value:
 Oueries value:
                         HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[type]
 Oueries value:
                         HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[guid]
                         HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[datatype0]
 Queries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[data0]
 Oueries value:
                         HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[action]
 Queries value:
 Oueries value:
                         HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[type]
 Oueries value:
                         HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[guid]
 Oueries value:
                         HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[datatype0]
 Queries value:
                         HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[data0]
 Oueries value:
                         HKLM \setminus system \setminus current control set \setminus services \setminus ikeext \setminus trigger in fo \setminus 0 \ [data type 1]
 Queries value:
                         HKLM\system\currentcontrolset\services\ikeext[imagepath]
 Oueries value:
                         HKLM\svstem\currentcontrolset\services\ikeext[tvpe]
 Oueries value:
                         HKLM\system\currentcontrolset\services\ikeext[start]
 Oueries value:
                         HKLM\system\currentcontrolset\services\ikeext[errorcontrol]
 Oueries value:
                         HKLM\system\currentcontrolset\services\ikeext[tag]
 Oueries value:
                         HKLM\system\currentcontrolset\services\ikeext[dependonservice]
 Queries value:
                         HKLM\system\currentcontrolset\services\ikeext[dependongroup]
 Oueries value:
                         HKLM\system\currentcontrolset\services\ikeext[group]
 Queries value:
                         HKLM\system\currentcontrolset\services\ikeext[objectname]
 Oueries value:
                         HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[action]
 Oueries value:
                         HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[type]
 Oueries value:
                         HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[guid]
                         HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[datatype0]
 Queries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[action]
 Oueries value:
                         HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[guid]
 Queries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[datatype0]
 Oueries value:
                         HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[action]
                         HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[type]
 Oueries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[guid]
 Oueries value:
                         Queries value:
                         HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a66e19e6]
 Oueries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
HKLM\software\microsoft\samclient\windows\disabledsessions[globalsession1
 Queries value:
                         HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[action]
 Queries value:
                         HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[type]
 Oueries value:
                         HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[guid]
 Queries value:
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype0]
                         HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[data0]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype1]
 Oueries value:
                         HKLM\system\currentcontrolset\services\policyagent[imagepath]
```

HKLM\system\currentcontrolset\services\policyagent[type]

HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype2]

Oueries value:

Queries value:

```
Oueries value:
                                   HKLM\system\currentcontrolset\services\policyagent[start]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\policyagent[errorcontrol]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\policyagent[tag]
                                   HKLM\system\currentcontrolset\services\policyagent[dependonservice]
  Queries value:
  Oueries value:
                                   HKLM\system\currentcontrolset\services\policyagent[dependongroup]
  Queries value:
                                   HKLM\system\currentcontrolset\services\policyagent[group]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\policyagent[objectname]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[action]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[type]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[guid]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[datatype0]
  Queries value:
                                   HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[action]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[type]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[guid]
  Queries value:
                                   HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[datatype0]
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus trigger in fo \setminus 0 \ [action]
  Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[type]
  Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[guid]
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus table tinput service \setminus trigger in fo \setminus 0 \ [data type 0]
  Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data0]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus table tinput service \setminus trigger in fo \setminus 0 [data type 1]
  Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data1]
  Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype2]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus table tinput service \setminus trigger in fo \setminus 0 \ [data 2]
  Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data3]
  Oueries value:
HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[action]
  Queries value:
  Oueries value:
                                   HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[type]
  Queries value:
                                   HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[guid]
  Queries value:
                                   HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[datatype0]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[action]
                                   HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[type]
  Oueries value:
  Queries value:
                                   HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[guid]
  Oueries value:
                                   Queries value:
                                   HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[action]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[type]
  Queries value:
                                   HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[guid]
  Oueries value:
HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[datatype0]
                                   HKLM \verb|\system| current controlset \verb|\services| wersvc \verb|\triggerinfo| 0 [action]|
  Queries value:
  Queries value:
                                   HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[type]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[guid]
  Queries value:
                                   HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[datatype0]
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[action]
  Oueries value:
  Queries value:
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[type]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[guid]
  Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[datatype0]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[type]
  Queries value:
  Queries value:
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[guid]
  Oueries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[datatype0]
  Queries value:
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[action]
  Oueries value:
                                   \label{lem:hklmsystem} HKLM \system \current controlset \services \wpdbusenum \triggerinfo \cite{type} \]
  Queries value:
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[guid]
  Oueries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[datatype0]
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[action]
  Oueries value:
  Oueries value:
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[type]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[guid]
  Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[datatype0]
                                   HKLM \verb|\system| current controlset \verb|\services| \verb|\wudfsvc| trigger info \verb|\oldownormal| of the controlset \verb|\system| current controlset c
  Queries value:
                                   HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[type]
  Oueries value:
  Oueries value:
                                   HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[guid]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype0]
  Queries value:
                                   HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[data0]
```

HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype1]

HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}[]

Queries value: Queries value:

Oueries value: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32[inprocserver32] Queries value: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32[] Queries value: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32[threadingmodel] Queries value: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}[] Oueries value: HKCR\clsid\{a2a9545d-a0c2-42b4-9708a0b2badd77c8}\inprocserver32[inprocserver32] HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprocserver32[] Queries value: Oueries value: HKCR\clsid\{a2a9545d-a0c2-42b4-9708a0b2badd77c8}\inprocserver32[threadingmodel] HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}[] Queries value: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-Queries value: 535773d48449}\inprocserver32[inprocserver32] HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprocserver32[] Queries value: Oueries value: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprocserver32[threadingmodel] HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}[] Queries value: HKCR\clsid\{dd313e04-feff-11d1-8ecd-Queries value: 0000f87a470c}\inprocserver32[inprocserver32] HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32[] Queries value: Queries value: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32[threadingmodel] 9926f41749ea}\count[{q6523100-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr] $HKCU \setminus software \setminus classes \setminus clsid \setminus \{fbeb8a05-beee-4442-804e-beee-4444-beee-4440-beee-440-be$ Sets/Creates value: 409d6c4515e9}\inprocserver32[threadingmodel] HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-Sets/Creates value: 409d6c4515e9}\inprocserver32[] HKLM\software\microsoft\direct3d\mostrecentapplication[name] Value changes: Value changes: HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32[] Value changes: Value changes: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ catalog_entries \ 000000000017 \ [packed catalog item]$ Value changes: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ catalog_entries \ 0000000000016 \ [packed catalog item]$ Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem] Value changes: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ catalog_entries \ 000000000014 \ [packed catalog item]$ Value changes: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ catalog_entries \ 0000000000013 \ [packed catalog item]$ Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem] Value changes: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ catalog_entries \ 0000000000011 \ [packed catalog item]$ Value changes: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ catalog_entries \ 0000000000010 \ [packed catalog item]$ Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem] HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000008[packedcatalogitem] Value changes: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ catalog_entries \ 0000000000007 \ [packed catalog item]$ Value changes: Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem] Value changes: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ catalog_entries \ 000000000004 \ [packed catalog item]$ 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: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ catalog_entries \ 000000000001 \ [packed catalog item]$ Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[librarypath] Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath] Value changes: HKLM\system\currentcontrolset\services\browser[start] Value changes: HKLM\system\currentcontrolset\services\policyagent[start] Value changes: HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-9926f41749ea}\count[{q65231o0-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]

HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-

9926f41749ea}\count[hrzr_pgyfrffvba]