Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3329, Task ID: 826

Task ID: 826 Risk Level: 10

Date Processed: 2016-05-18 10:42:32 (UTC)

Processing Time: 62.56 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\26ec828da6d2651f90c74cb275b800cc.exe"

Sample ID: Type: basic Owner: admin

26ec828da6d2651f90c74cb275b800cc Label: Date Added:

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

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

26ec828da6d2651f90c74cb275b800cc MD5:

2fd94a7ba79df111cbd03365c4ae7ccc17e7dfaba10a30ed3049db2f369c2d4b SHA256:

Description: None

Pattern Matching Results

6 Modifies registry autorun entries

- Writes to memory of system processes
- 6 Writes to system32 folder
- 5 Abnormal sleep detected
- 5 Installs service
- 3 Connects to local host
- 6 Changes Winsock providers
- 10 Creates malicious events: ZeroAccess [Rootkit]
- 4 Reads process memory
- 3 Long sleep detected
- 7 Injects thread into Windows process

Process/Thread Events

C:\windows\temp\26ec828da6d2651f90c74cb275b800cc.exe

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

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

bfe.dll,BfeOnServiceStartTypeChange]

Creates process: C:\Windows\system32\sppsvc.exe [C:\Windows\system32\sppsvc.exe] Creates process: C:\Program Files\Windows Media Player\wmpnetwk.exe ["C:\Program

Files\Windows Media Player\wmpnetwk.exe"]

PID:2904 C:\Windows\Temp\26ec828da6d2651f90c74cb275b800cc.exe Reads from process:

Reads from process: PID:2076 C:\Windows\SysWOW64\calc.exe

PID:2904 C:\Windows\Temp\26ec828da6d2651f90c74cb275b800cc.exe Writes to process:

PID:340 C:\Windows\explorer.exe Writes to process:

Writes to process: PID:436 C:\Windows\System32\services.exe Writes to process: PID:2132 C:\Windows\System32\sppsvc.exe

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

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

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

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex: \BaseNamedObjects\DBWinMutex

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

\BaseNamedObjects\SvcctrlStartEvent_A3752DX Creates events

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

\BaseNamedObjects\{9E1C6465-1D54-4446-9F99-8639AF243513} Creates event: \KernelObjects\MaximumCommitCondition Creates event:

 $\verb|\Sessions|1| BaseNamedObjects| PRS_EXTERNAL_CHECK_CHANGED_NOTIFY| \\$ Creates event: \Sessions\1\BaseNamedObjects\{43a2b8d7-6fed-4c18-bd36-b4630d61afb5}

File System Events

C:\\$Recycle.Bin\ Creates

Creates: C:\\$Recvcle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001 C:\\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-Creates:

1001\\$aaa1415b79b8dbbd8bd16c842c1858a2

C:\\$Recvcle.Bin\S-1-5-21-980053277-1733835069-2361817685-Creates:

1001\\$aaa1415b79b8dbbd8bd16c842c1858a2\L

C:\\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-Creates:

1001\\$aaa1415b79b8dbbd8bd16c842c1858a2\U

C:\\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-

1001\\$aaa1415b79b8dbbd8bd16c842c1858a2\@

```
1001\$aaa1415b79b8dbbd8bd16c842c1858a2\n
  Creates:
                                       C:\Program Files\Windows Defender\en-US:!
                                       C:\Program Files\Windows Defender\MpAsDesc.dll:!
  Creates:
                                       C:\Program Files\Windows Defender\MpClient.dll:!
  Creates:
  Creates:
                                       C:\Program Files\Windows Defender\MpCmdRun.exe:!
                                       C:\Program Files\Windows Defender\MpCommu.dll:!
  Creates:
                                       C:\Program Files\Windows Defender\MpEvMsg.dll:!
  Creates:
  Creates:
                                       C:\Program Files\Windows Defender\MpOAV.dll:!
  Creates:
                                       C:\Program Files\Windows Defender\MpRTP.dll:!
                                       C:\Program Files\Windows Defender\MpSvc.dll:!
  Creates:
  Creates:
                                       C:\Program Files\Windows Defender\MSASCui.exe:!
  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\$aaa1415b79b8dbbd8bd16c842c1858a2
  Creates:
  Creates:
                                       C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\L
  Creates:
                                       C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\U
                                       C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\@
  Creates:
  Creates:
                                       C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\n
  Creates:
                                       C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001\$I5D1DD46B
                                       C:GAC_MSIL
  Creates:
  Creates:
                                       C:GAC
  Creates:
                                       C:GAC_32
                                       C:GAC 64
  Creates:
                                       C:\Windows\assembly\GAC_64\Desktop.ini
  Creates:
  Creates:
                                       C:\Windows\assembly\GAC_32\Desktop.ini
                                       C:\Windows\System32\LogFiles\Scm\e22a8667-f75b-4ba9-ba46-067ed4429de8
  Creates:
                                       C:\Windows\System32\LogFiles\Scm\9435f817-fed2-454e-88cd-7f78fda62c48
  Creates:
  Creates:
                                       C:\Windows\system32\catroot
  Creates:
                                       C:\Windows\system32\catroot2
                                       C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft
  Creates:
  Creates:
C: \verb|\windows| Service Profiles \end{| Network Service AppData Local Microsoft \end{| Windows Media Player NSS \end{| Network Service No. 1000 and No. 1000 and
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player
NSS\3.0\SCPD
  Creates
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player
NSS\3.0\Icon Files
                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\WER\ERC
  Creates:
  Creates:
                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\WER\ERC\statecache.lock
  Opens:
                                       C:\Windows\Prefetch\26EC828DA6D2651F90C74CB275B80-7FC87F1F.pf
  Opens:
                                       C:\Windows
  Opens:
                                       C:\Windows\System32\wow64.dll
                                       C:\Windows\System32\wow64win.dll
  Opens:
  Opens:
                                       C:\Windows\System32\wow64cpu.dll
                                       C:\Windows\system32\wow64log.dll
  Opens:
  Opens:
                                       C:\Windows\SysWOW64
  Opens:
                                       C:\Windows\SysWOW64\sechost.dll
  Opens:
                                       C:\windows\temp\D3D8.DLL
  Opens:
                                       C:\Windows\SysWOW64\d3d8.dll
  Opens:
                                       C:\windows\temp\VERSION.dll
  Opens:
                                       C:\Windows\SysWOW64\version.dll
  Opens:
                                       C:\windows\temp\d3d8thk.dll
  Opens:
                                       C:\Windows\SysWOW64\d3d8thk.dll
  Opens:
                                       C:\windows\temp\dwmapi.dll
                                       C:\Windows\SysWOW64\dwmapi.dll
  Opens:
  Opens:
                                       C:\windows\temp\opengl32.dll
  Opens:
                                       C:\Windows\SysWOW64\opengl32.dll
  Opens:
                                       C:\windows\temp\GLU32.dll
  Opens:
                                       C:\Windows\SysWOW64\glu32.dll
  Opens:
                                       C:\windows\temp\DDRAW.dll
                                       C:\Windows\SysWOW64\ddraw.dll
  Opens:
  Opens:
                                       C:\windows\temp\DCIMAN32.dll
  Opens:
                                       C:\Windows\SysWOW64\dciman32.dll
  Opens:
                                       C:\Windows\SysWOW64\imm32.dll
  Opens:
                                       C:\Windows\SysWOW64\en-US\setupapi.dll.mui
  Opens:
                                       C:\windows\temp\MSCAT32.dll
                                       C:\Windows\SysWOW64\mscat32.dll
  Opens:
  Opens:
                                       C:\Windows\Temp\26ec828da6d2651f90c74cb275b800cc.exe
  Opens:
                                       C:\Windows\SysWOW64\apphelp.dll
  Opens:
                                       C:\Windows\System32\ntdll.dll
  Opens:
                                       C:\Windows\SysWOW64\ntdll.dll
                                       C:\Windows\System32\kernel32.dll
  Opens:
  Opens:
                                       C:\Windows\SysWOW64\kernel32.dll
  Opens:
                                       C:\Windows\System32\user32.dll
  Opens:
                                       C:\Windows\SysWOW64\KernelBase.dll
  Opens:
                                       C:\Windows\SysWOW64\user32.dll
  Opens:
                                       C:\Windows\SysWOW64\gdi32.dll
                                       C:\Windows\SysWOW64\landle{lpk.dll}
  Opens:
  Opens:
                                       C:\Windows\SysWOW64\usp10.dll
```

C:\\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-

Creates:

```
C:\Windows\SysWOW64\msvcrt.dll
 Opens:
                         C:\Windows\SysWOW64\advapi32.dll
                         C:\Windows\SysWOW64\rpcrt4.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\sspicli.dll
 Opens:
                         C:\Windows\SysWOW64\cryptbase.dll
 Opens:
                         C:\Windows\SysWOW64\setupapi.dll
 Opens:
                         C:\Windows\SysWOW64\cfgmgr32.dll
                         C:\Windows\SysWOW64\oleaut32.dll
 Opens:
                         C:\Windows\SysWOW64\ole32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\devobj.dll
 Opens:
                         C:\Windows\SysWOW64\msctf.dll
 Opens:
                         C:\Windows\SysWOW64\wintrust.dll
 Opens:
                         C:\Windows\SysWOW64\crypt32.dll
 Opens:
                         C:\Windows\SysWOW64\msasn1.dll
 Opens:
                         C:\windows\temp\untfs.dll
                         C:\Windows\SysWOW64\untfs.dll
 Opens:
 Opens:
                         C:\windows\temp\Cabinet.dll
 Opens:
                         C:\Windows\SysWOW64\cabinet.dll
 Opens:
                         C:\Windows\SysWOW64\ws2_32.dll
 Opens:
                         C:\Windows\SysWOW64\nsi.dll
 Opens:
                         C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens:
                         C:\Windows\SysWOW64\mswsock.dll
 Opens:
                         C:\Windows\SysWOW64\WSHTCPIP.DLL
 Opens:
                         C:\windows\temp\CRYPTSP.dll
 Opens:
                         C:\Windows\SysWOW64\cryptsp.dll
 Opens:
                         C:\Windows\SysWOW64\rsaenh.dll
 Opens:
                         C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-
1001\$aaa1415b79b8dbbd8bd16c842c1858a2\n
                         C:\Program Files\Windows Defender
 Opens:
 Opens:
                         C:\Program Files\Windows Defender\en-US
 Opens:
                         C:\Windows\MSWSOCK.dll
 Opens:
                         C:\Windows\System32\mswsock.dll
 Opens:
                         C:\Program Files\Windows Defender\MpAsDesc.dll
 Opens:
                         C:\Program Files\Windows Defender\MpClient.dll
 Opens:
                         C:\Program Files\Windows Defender\MpCmdRun.exe
 Opens:
                         C:\Program Files\Windows Defender\MpCommu.dll
 Opens:
                         C:\Program Files\Windows Defender\MpEvMsg.dll
 Opens:
                         C:\Program Files\Windows Defender\MpOAV.dll
 Opens:
                         C:\Program Files\Windows Defender\MpRTP.dll
 Opens:
                         C:\Program Files\Windows Defender\MpSvc.dll
 Opens:
                         C:\Program Files\Windows Defender\MSASCui.exe
 Opens:
                         C:\Program Files\Windows Defender\MsMpCom.dll
 Opens:
                         C:\Program Files\Windows Defender\MsMpLics.dll
 Opens:
                         C:\Program Files\Windows Defender\MsMpRes.dll
 Opens:
                         C:\Program Files\Microsoft Security Client
 Opens:
                         C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\n
                         C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001
 Opens:
 Opens:
                         C:\Windows\assembly
 Opens:
                         C:\Windows\assembly\GAC_32\Desktop.ini
                         C:\Windows\assembly\GAC_64\Desktop.ini
 Opens:
 Opens:
                         C:\Windows\System32\cryptsp.dll
 Opens:
                         C:\Windows\System32\rsaenh.dll
                         \label{lem:c:secycle.Bin\s-1-5-18} $$aaa1415b79b8dbbd8bd16c842c1858a2\\ @
 Opens:
 Opens:
                         C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\U
 Opens:
                         C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-
1001\$aaa1415b79b8dbbd8bd16c842c1858a2\@
 Opens:
                         C:\Windows\Temp
 Opens:
                         C:\Windows\System32\rundl132.exe
 Opens:
                         C:\Windows\Prefetch\RUNDLL32.EXE-39102DB5.pf
 Opens:
                         C:\Windows\System32
 Opens:
                         C:\Windows\System32\imm32.dll
 Opens:
                         C:\Windows\System32\en-US\rundll32.exe.mui
 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\sechost.dll
                         C:\Windows\System32\LogFiles\Scm\e22a8667-f75b-4ba9-ba46-067ed4429de8
 Opens:
 Opens:
                         C:\Windows\System32\Tasks\Microsoft\Windows\WDI\ResolutionHost
 Opens:
                         C:\Windows\SysWOW64\calc.exe
 Opens:
                         C:\
 Opens:
                         C:\Users\Admin\Desktop
 Opens:
                         C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp
                         C:\Windows\ServiceProfiles
 Opens:
 Opens:
                         C:\Windows\System32\sppsvc.exe
 Opens:
                         C:\Windows\AppPatch\AppPatch64\sysmain.sdb
 Opens:
                         C:\Windows\Prefetch\SPPSVC.EXE-B0F8131B.pf
 Opens:
                         C:\Windows\System32\en-US\sppsvc.exe.mui
 Opens:
                         C:\Windows\System32\rpcss.dll
 Opens:
                         C:\Windows\System32\cryptbase.dll
```

Opens:

```
C:\Windows\System32\RpcRtRemote.dll
 Opens:
 Opens:
                         C:\Program Files\Windows Media Player\wmpnetwk.exe
                         C:\Windows\Prefetch\WMPNETWK.EXE-D9F2A96F.pf
 Opens:
 Opens:
                         C:\Program Files\Windows Media Player\WSOCK32.dll
 Opens:
                         C:\Windows\System32\wsock32.dll
 Opens:
                         C:\Program Files\Windows Media Player\IPHLPAPI.DLL
 Opens:
                         C:\Windows\System32\IPHLPAPI.DLL
 Opens:
                         C:\Program Files\Windows Media Player\WINNSI.DLL
 Opens:
                         C:\Windows\System32\winnsi.dll
 Opens:
                         C:\Program Files\Windows Media Player\USERENV.dll
 Opens:
                         C:\Windows\System32\userenv.dll
 Opens:
                         C:\Program Files\Windows Media Player\profapi.dll
 Opens:
                         C:\Windows\System32\profapi.dll
                         C:\Program Files\Windows Media Player\WTSAPI32.dll
 Opens:
 Opens:
                         C:\Windows\System32\wtsapi32.dll
 Opens:
                         C:\Program Files\Windows Media Player\en-US\wmpnetwk.exe.mui
 Opens:
                         C:\Program Files\Windows Media Player\CRYPTBASE.dll
 Opens:
                         C:\Program Files\Windows Media Player\POWRPROF.DLL
 Opens:
                         C:\Windows\System32\powrprof.dll
 Opens:
                         C:\Windows\System32\en-US\setupapi.dll.mui
 Opens:
                         C:\Program Files\Windows Media Player\WINSTA.dll
 Opens:
                         C:\Windows\System32\winsta.dll
 Opens:
                         C:\Program Files\Windows Media Player\ntmarta.dll
 Opens:
                         C:\Windows\System32\ntmarta.dll
 Opens:
                         C:\Program Files\Windows Media Player\wmdrmdev.dll
 Opens:
                         C:\Windows\System32\wmdrmdev.dll
 Opens:
                         C:\Program Files\Windows Media Player\drmv2clt.dll
 Opens:
                         C:\Windows\System32\drmv2clt.dll
 Opens:
                         C:\Program Files\Windows Media Player\VERSION.dll
 Opens:
                         C:\Windows\System32\version.dll
 Opens:
                         C:\Program Files\Windows Media Player\MFPlat.DLL
 Opens:
                         C:\Windows\System32\mfplat.dll
 Opens:
                         C:\Program Files\Windows Media Player\AVRT.dll
 Opens:
                         C:\Windows\System32\avrt.dll
 Opens:
                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
 Opens:
                         C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
 Opens:
                         C:\Windows\System32\catroot
 Opens:
                         C:\Windows\System32\catroot2
 Opens:
                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package~31bf3856ad364e35~amd64~~6.1.7601.17514.cat
                         C:\ProgramData\Microsoft\Windows\DRM
 Opens:
 Opens:
                         C:\ProgramData\Microsoft\Windows\DRM\drmstore.hds
 Opens:
                         C:\ProgramData\Microsoft\Windows\DRM\v3ks.bla
 Opens:
                         C:\Windows\System32\blackbox.dll
 Opens:
                         C:\ProgramData\Microsoft\Windows\DRM\blackbox.bin
 Opens:
                         C:\ProgramData\Microsoft\Windows\DRM\v3ks.sec
                         C:\Windows\ServiceProfiles\NetworkService\AppData\Local
 Opens:
 Opens:
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player NSS\3.0
 Opens:
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player NSS
{\tt C:\Windows\Service\Profiles\Network\Service\AppData\Local\Microsoft\Windows\ Media\ Player}
NSS\3.0\Icon Files
 Opens:
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player
NSS\3.0\SCPD
                         C:\Program Files\Windows Media Player\CRYPTSP.dll
 Opens:
                         C:\Windows\System32\wscinterop.dll
 Opens:
 Opens:
                         C:\Windows\System32\wscapi.dll
 Opens:
                         C:\Windows\System32\wscui.cpl
 Opens:
                         C:\Windows\System32\wscinterop.dll.123.Manifest
 Opens:
                         C:\Windows\System32\en-US\wscui.cpl.mui
 Opens:
                         C:\Program Files\Windows Media Player\RpcRtRemote.dll
 Opens:
                         C:\Windows\System32\werconcpl.dll
 Opens:
                         C:\Windows\System32\framedynos.dll
 Opens:
                         C:\Windows\System32\wercplsupport.dll
 Opens:
                         C:\Windows\System32\upnp.dll
 Opens:
                         C:\Users\Admin\AppData\Local
 Opens:
                         C:\Windows\System32\winhttp.dll
                         C:\Windows\System32\webio.dll
 Opens:
 Opens:
                         C:\Windows\System32\ssdpapi.dll
                         C:\Windows\System32\msxml6.dll
 Opens:
                         C:\Windows\System32\en-US\KernelBase.dll.mui
 Opens:
 Opens:
                         C:\Windows\System32\msxml6r.dll
 Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\WER\ReportArchive
 Opens:
 Opens:
                         C:\ProgramData\Microsoft\Windows\WER\ReportArchive
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\WER\ERC
 Opens:
                         C:\Program Files\Windows Media Player\SXS.DLL
 Opens:
                         C:\Windows\Svstem32\sxs.dll
 Opens:
                         C: \verb|\USers\Admin\AppData\Local\Microsoft\Windows\WER\ERC\queuepester.txt|
```

C:\Windows\System32\stdole2.tlb Opens: C:\Windows\System32\hcproviders.dll Opens: Opens: C:\Windows\Explorer.EXE.Local\ C:\Windows\winsxs\amd64_microsoft.windows.common-Opens: controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9ac Opens: C:\Windows\System32\en-US\hcproviders.dll.mui Opens: C:\Windows\System32\en-US\ActionCenter.dll.mui Opens: C:\Program Files\Internet Explorer\ieproxy.dll C:\\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-Writes to: 1001\\$aaa1415b79b8dbbd8bd16c842c1858a2\@ C:\\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-Writes to: 1001\\$aaa1415b79b8dbbd8bd16c842c1858a2\n Writes to: C:\\$Recycle.Bin\S-1-5-18\\$aaa1415b79b8dbbd8bd16c842c1858a2\@ C:\\$Recycle.Bin\S-1-5-18\\$aaa1415b79b8dbbd8bd16c842c1858a2\n Writes to: Writes to: C:\Windows\assembly\GAC_64\Desktop.ini C:\\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001\\$I5D1DD46B Writes to: C:\Windows\assembly\GAC_32\Desktop.ini Writes to: Writes to: C:\Windows\System32\LogFiles\Scm\e22a8667-f75b-4ba9-ba46-067ed4429de8 Writes to: C:\Windows\System32\LogFiles\Scm\9435f817-fed2-454e-88cd-7f78fda62c48 Reads from: C:\Windows\Temp\26ec828da6d2651f90c74cb275b800cc.exe Reads from: C:\\$Recycle.Bin\S-1-5-18\\$aaa1415b79b8dbbd8bd16c842c1858a2\@ C:\Windows\System32\LogFiles\Scm\e22a8667-f75b-4ba9-ba46-067ed4429de8 Reads from: Reads from: C:\ProgramData\Microsoft\Windows\DRM\drmstore.hds Reads from: C:\ProgramData\Microsoft\Windows\DRM\blackbox.bin Reads from: C:\ProgramData\Microsoft\Windows\DRM\v3ks.sec Reads from: C:\ProgramData\Microsoft\Windows\DRM\v3ks.bla Reads from: C:\Windows\System32\upnp.dll

 $C: \verb|\windows\Temp\26ec828da6d2651f90c74cb275b800cc.exe| \\$

C:\Windows\System32\stdole2.tlb

Network Events

Reads from:

Deletes:

DNS query:	j.maxmind.com
DNS query. 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:	206.254.253.254:16470
Sends data to:	197.254.253.254:16470
Sends data to:	190.254.253.254:16470
Sends data to:	184.254.253.254:16470
Sends data to:	183.254.253.254:16470
Sends data to:	182.254.253.254:16470
Sends data to:	180.254.253.254:16470
Sends data to:	166.254.253.254:16470
Sends data to:	158.254.253.254:16470
Sends data to:	135.254.253.254:16470
Sends data to:	134.254.253.254:16470
Sends data to:	119.254.253.254:16470
Sends data to:	117.254.253.254:16470
Sends data to:	115.254.253.254:16470
Sends data to:	113.254.253.254:16470
Sends data to:	69.121.230.254:16470
Sends data to:	1.186.134.249:16470
Sends data to:	193.30.251.248:16470
Sends data to:	2.192.37.245:16470
Sends data to:	117.109.27.245:16470
Sends data to:	49.205.25.244:16470
Sends data to:	75.65.128.242:16470
Sends data to:	71.206.79.242:16470
Sends data to:	76.94.226.239:16470
Sends data to:	66.66.109.239:16470
Sends data to:	98.143.7.239:16470
Sends data to:	188.25.115.238:16470
Sends data to:	69.141.58.238:16470
Sends data to:	137.186.139.237:16470
Sends data to:	174.4.174.236:16470
Sends data to:	24.21.90.235:16470
Sends data to:	78.84.103.234:16470
Sends data to:	74.115.1.233:16470
Sends data to:	24.144.182.232:16470
Sends data to:	88.68.214.231:16470
Sends data to:	87.72.8.231:16470
Sends data to:	82.235.17.230:16470
Sends data to:	69.31.207.228:16470
Receives data from:	0.0.0.0:0

Windows Registry Events

Creates key: HKLM\software\www6432node\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

```
Creates kev:
                                              HKLM\system\currentcontrolset\services\eventlog\system\wmpnetworksvc
                                              HKLM\system
   Creates kev:
                                              HKLM\system\currentcontrolset
   Creates kev:
                                              HKLM\system\currentcontrolset\services
   Creates key:
   Creates kev:
                                              HKLM\system\currentcontrolset\services\eventlog
   Creates key:
                                              HKLM\system\currentcontrolset\services\eventlog\system
                                              HKLM\software\microsoft\windows media player nss\3.0\events
   Creates kev:
                                              \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \software \microsoft \windows media player nss \3.0 \events \end{tabular} $$ \{9e1c6465-events \end{tabular} $$ \{9e1c6
   Creates key:
1d54-4446-9f99-8639af243513}
                                              HKLM\software\microsoft\cryptography\rng
   Creates key:
   Creates key:
                                              HKLM\software\microsoft\windows media player nss\3.0\devices\00-00-00-
00-00-00
  Creates key:
                                              HKLM\software\microsoft\windows media player nss\3.0\devices\08-00-27-
e8-14-9e
   Creates key:
                                              HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.106
                                              HKCU\software\microsoft\windows\currentversion\action
  Creates key:
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.101
  Creates key:
                                              HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.103
   Creates key:
                                              HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.100
                                              HKCU\software\microsoft\windows\currentversion\action
  Creates key:
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.102
  Creates key:
                                              HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.104
                                              HKCU\software\microsoft\windows\currentversion\action
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.100
   Creates kev:
                                              HKCU\software\microsoft\windows\windows error reporting
   Creates key:
                                              HKCU\software\microsoft\windows\currentversion\action
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2\}.check.101
                                              HKCU\software\microsoft\windows\currentversion\action
  Creates key:
center\checks\{c8e6f269-b90a-4053-a3be-499afcec98c4}.check.0
   Creates key:
                                              HKCU\software\microsoft\windows\currentversion\action
center \verb|\providers| eventlog \verb|\footnotemark| \{01979c6a-42fa-414c-b8aa-eee2c8202018\}
                                              HKCU\software\microsoft\windows\currentversion\action
center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.100
                                              HKCU\software\microsoft\windows\currentversion\action
  Creates key:
center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.101
                                              HKCU\software\microsoft\windows\currentversion\action
   Creates key:
center \verb|\providers| eventlog \verb|\{945a8954-c147-4acd-923f-40c45405a658\}| 
                                             HKCU\software\microsoft\windows\currentversion\action
   Creates key:
center\checks\{945a8954-c147-4acd-923f-40c45405a658}.check.42
                                              HKCU\software\microsoft\windows\currentversion\action
  Creates key:
center\providers\eventlog\{dab69a6a-4d2a-4d44-94bf-e0091898c881}
                                              HKCU\software\microsoft\windows\currentversion\action
   Creates key:
center\checks\{dab69a6a-4d2a-4d44-94bf-e0091898c881}.check.100
                                              HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}
                                              \label{lem:hklmsoftware} \verb+ HKLM \software \microsoft \windows \current version \normalisation \normalisation
   Deletes value:
   Opens key:
                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options
   Opens key:
                                              HKLM\system\currentcontrolset\control\session manager
   Opens key:
                                              HKLM\software\microsoft\wow64
   Opens key:
                                              HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
   Opens key:
                                              HKLM\system\currentcontrolset\control\terminal server
   Opens key:
                                              HKLM\system\currentcontrolset\control\safeboot\option
                                              HKLM\system\currentcontrolset\control\srp\gp\dll
   Opens kev:
   Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
   Opens key:
                                              HKLM\software\policies\microsoft\windows\safer\codeidentifiers
   Opens key:
                                              HKCU\software\policies\microsoft\windows\safer\codeidentifiers
   Opens key:
                                              HKLM\system\currentcontrolset\control\nls\customlocale
                                              HKLM\system\currentcontrolset\control\nls\language
   Opens key:
   Opens key:
                                              HKLM\system\currentcontrolset\control\mui\uilanguages
   Opens key:
                                              HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
   Opens key:
                                              HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
   Opens key:
                                              HKLM\software\wow6432node\policies\microsoft\mui\settings
   Opens key:
                                              HKLM\software\policies\microsoft\mui\settings
   Opens key:
   Opens key:
                                              HKCU\control panel\desktop\muicached\machinelanguageconfiguration
   Opens key:
                                              HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
                                              HKCU\software\policies\microsoft\control panel\desktop
   Opens key:
   Opens key:
                                              HKCU\control panel\desktop\languageconfiguration
                                              HKCU\control panel\desktop
   Opens kev:
                                              HKCU\control panel\desktop\muicached
   Opens key:
   Opens key:
                                              HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
   Opens key:
                                              HKLM\system\currentcontrolset\control\nls\sorting\versions
   Opens kev:
                                              HKLM\
   Opens key:
                                              HKLM\software\wow6432node\microsoft\windows
```

nt\currentversion\diagnostics

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\gre_initialize HKLM\software\wow6432node\microsoft\windows Opens kev: nt\currentversion\compatibility32 Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime compatibility Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ nt \ current version \ windows$ Opens key: HKLM\software\wow6432node\microsoft\direct3d Opens key: HKLM\software\policies\microsoft\sqmclient\windows Opens key: HKLM\software\microsoft\sqmclient\windows Opens key: HKLM\software\wow6432node\microsoft\ole HKLM\software\wow6432node\microsoft\ole\tracing Opens key: Opens key: HKLM\software\microsoft\ole\tracing Opens key: HKLM\software\wow6432node\microsoft\oleaut Opens key: HKLM\system\currentcontrolset\control\cmf\config Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\setup Opens key: HKLM\software\microsoft\windows\currentversion\setup Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion Opens key: Opens key: HKLM\system\currentcontrolset\services\crypt32 Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\msasn1 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\26ec828da6d2651f90c74cb275b800cc.exe Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility Opens key: HKLM\software\wow6432node\policies\microsoft\windows\appcompat Opens key: HKLM\software\policies\microsoft\windows\appcompat Opens key: HKCU\software\microsoft\windows nt\currentversion HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers Opens key: Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\appcompatflags HKLM\software\wow6432node\microsoft\windows Opens key: nt\currentversion\appcompatflags\custom\26ec828da6d2651f90c74cb275b800cc.exe Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wow64win.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\wow64cpu.dll $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ Opens key: options\wow64.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernelbase.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution $options \verb|\usp10.dll|$ Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution $options \verb|\lpk.dll|$ 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\cryptbase.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\sspicli.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rpcrt4.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\sechost.dll $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ Opens key: options\advapi32.dll Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$ options\user32.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: options\msctf.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\imm32.dll Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$ options\version.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: options\d3d8thk.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dwmapi.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\d3d8.dll

HKLM\software\microsoft\windows nt\currentversion\image file execution

HKLM\software\microsoft\windows nt\currentversion\image file execution

HKLM\software\microsoft\windows nt\currentversion\image file execution

HKLM\software\microsoft\windows nt\currentversion\image file execution

Opens key:

options\glu32.dll Opens key:

options\dciman32.dll
 Opens key:

options\cfgmgr32.dll
 Opens key:

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 HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: 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 HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: 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 HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: options\mscat32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\cabinet.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\nsi.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: options\ws2_32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\136a17c6 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries Opens kev: Opens key: Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005 Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008 Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010 Opens key: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5$ Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006 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\tcpip\parameters\winsock Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers 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

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

options\cryptsp.dll

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ cryptography \ defaults \ provider \ microsoft \ base \ cryptographic$

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

Opens key: HKLM\system\currentcontrolset\control\lsa

Opens key:

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

HKLM\software\microsoft\cryptography Opens key:

Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload

Opens key:

HKLM\software\wow6432node\microsoft\cryptography\deshashsessionkeybackward Opens key: HKLM\system\currentcontrolset\services\windefend

Opens key: HKLM\system\currentcontrolset\services\windefend\parameters Opens key: HKLM\system\currentcontrolset\services\windefend\security Opens key: HKLM\system\currentcontrolset\services\windefend\triggerinfo Opens key: HKLM\system\currentcontrolset\services\windefend\triggerinfo\0

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\shellserviceobjects\{fd6905ce-952f-41f1-9a6f-135d9c6622cc}

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ shells ervice objects \ \ \{f56f6fdd-fine \ for the constant \ for the \ for$ aa9d-4618-a949-c1b91af43b1a}

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus run$ Opens kev:

Opens key: HKLM\software\wow6432node\microsoft\rpc

Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername

HKLM\system\setup Opens key:

Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc

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

Opens key: HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32

Opens key:

Opens key:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\0000000000006 Opens key:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\0000000000003

Opens key:

Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001

Opens kev:

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000005 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000003 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000000 Opens key:

Opens key: $HKLM \ software \ microsoft \ base$

cryptographic provider v1.0

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

Opens key: $HKLM \backslash software \backslash microsoft \backslash cryptography \backslash deshash session keybackward$ Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist Opens key: HKLM\system\currentcontrolset\control\session manager\environment

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-18 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

HKU\.default\volatile environment Opens kev: 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\rundl132.exe

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

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

Opens key: HKU\.default\software\policies\microsoft\control panel\desktop
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: HKLM\system\currentcontrolset\control\error message instrument\
Opens key: HKLM\system\currentcontrolset\control\error message instrument
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility

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

Opens key: HKLM\software\microsoft\rpc

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

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

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

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

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

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

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

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

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

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
Opens key: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\bfe\triggerinfo

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

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

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

Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo\2

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

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

Opens key: HKLM\system\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:

 $HKLM \setminus system \setminus current control set \setminus services \setminus clr_optimization_v2.0.50727_32 \setminus triggerin fo$

Opens key: HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64

Opens key:

 $HKLM \setminus system \setminus current control set \setminus services \setminus clr_optimization_v2.0.50727_64 \setminus triggerin for the system \setminus system \setminus$

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

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

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

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

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

 $Opens~key: \\ HKLM\system\currentcontrolset\services\defragsvc\triggerinfo$

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

HKLM\system\currentcontrolset\services\dot3svc\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\dps Opens kev: HKLM\system\currentcontrolset\services\dps\triggerinfo HKLM\system\currentcontrolset\services\eaphost Opens key: Opens kev: HKLM\system\currentcontrolset\services\eaphost\triggerinfo Opens key: HKLM\system\currentcontrolset\services\efs HKLM\system\currentcontrolset\services\efs\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\efs\triggerinfo\0 Opens key: HKLM\system\currentcontrolset\services\efs\triggerinfo\1 HKLM\system\currentcontrolset\services\ehrecvr Opens key: Opens key: HKLM\system\currentcontrolset\services\ehrecvr\triggerinfo Opens key: ${\it HKLM \ } system \ `current control set \ `services \ `ehsched"$ Opens key: ${\tt HKLM \ } system \verb| current control set \verb| services \verb| ehsched \verb| trigger info \\$ 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 kev: Opens key: HKLM\system\currentcontrolset\services\fax Opens key: HKLM\system\currentcontrolset\services\fax\triggerinfo HKLM\system\currentcontrolset\services\fdphost Opens key: Opens key: HKLM\system\currentcontrolset\services\fdphost\triggerinfo HKLM\system\currentcontrolset\services\fdrespub Opens key: HKLM\system\currentcontrolset\services\fdrespub\triggerinfo Opens kev: Opens key: HKLM\system\currentcontrolset\services\fontcache Opens key: HKLM\system\currentcontrolset\services\fontcache\triggerinfo Opens key: $HKLM \setminus system \setminus current control set \setminus services \setminus font cache 3.0.0.0$ 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 HKLM\system\currentcontrolset\services\hkmsvc\triggerinfo Opens key: Opens key: ${\tt HKLM \ } system \verb| current control set \verb| services \verb| homegroup listener \\$ Opens key: HKLM\system\currentcontrolset\services\homegrouplistener\triggerinfo HKLM\system\currentcontrolset\services\homegroupprovider Opens key: Opens key: HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo Opens key: HKLM\system\currentcontrolset\services\idsvc HKLM\system\currentcontrolset\services\idsvc\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\ikeext Opens key: HKLM\system\currentcontrolset\services\ikeext\triggerinfo HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0 Opens key: Opens key: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\1 Opens key: HKLM\system\currentcontrolset\services\ipbusenum $\label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ services \+ ipbus en um \+ trigger in fo$ Opens key: Opens key: HKLM\system\currentcontrolset\services\ivmservice HKLM\system\currentcontrolset\services\keyiso Opens kev: HKLM\system\currentcontrolset\services\keyiso\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\ktmrm Opens key: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo $HKLM \verb|\system| current control set \verb|\services| ktmrm \verb|\triggerinfo|| 0$ Opens key: Opens key: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\1 Opens kev: HKLM\system\currentcontrolset\services\lanmanserver HKLM\system\currentcontrolset\services\lanmanserver\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\lanmanworkstation Opens key: HKLM\system\currentcontrolset\services\lanmanworkstation\triggerinfo HKLM\system\currentcontrolset\services\lltdsvc Opens key: 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: Opens key: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1 HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2 Opens key: Opens key: HKLM\system\currentcontrolset\services\mcx2svc Opens key: HKLM\system\currentcontrolset\services\mcx2svc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\mmcss Opens key: HKLM\system\currentcontrolset\services\mmcss\triggerinfo Opens key: HKLM\system\currentcontrolset\services\msdtc HKLM\system\currentcontrolset\services\msdtc\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\msiscsi Opens key: HKLM\system\currentcontrolset\services\msiscsi\triggerinfo Opens key: HKLM\system\currentcontrolset\services\msiserver Opens key: HKLM\system\currentcontrolset\services\msiserver\triggerinfo HKLM\system\currentcontrolset\services\napagent Opens kev: ${\it HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ napagent \verb|\ trigger info|$ Opens key: Opens key: HKLM\system\currentcontrolset\services\netlogon Opens key: HKLM\system\currentcontrolset\services\netlogon\triggerinfo Opens key: HKLM\software\microsoft\sqmclient\windows\disabledprocesses\ Opens key: HKLM\software\microsoft\sqmclient\windows\disabledsessions\ Opens kev: HKLM\svstem\currentcontrolset\services\netman

HKLM\system\currentcontrolset\services\netman\triggerinfo

Opens key:

HKLM\system\currentcontrolset\services\netprofm Opens key: HKLM\system\currentcontrolset\services\netprofm\triggerinfo Opens key: Opens kev: HKLM\system\currentcontrolset\services\nettcpportsharing HKLM\system\currentcontrolset\services\nettcpportsharing\triggerinfo Opens key: Opens kev: HKLM\svstem\currentcontrolset\services\nlasvc Opens key: HKLM\system\currentcontrolset\services\nlasvc\triggerinfo HKLM\system\currentcontrolset\services\nsi Opens key: Opens key: HKLM\system\currentcontrolset\services\nsi\triggerinfo Opens key: HKLM\system\currentcontrolset\services\ose HKLM\system\currentcontrolset\services\ose\triggerinfo Opens key: HKLM\system\currentcontrolset\services\p2pimsvc Opens key: Opens key: HKLM\system\currentcontrolset\services\p2pimsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\p2psvc HKLM\system\currentcontrolset\services\p2psvc\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\pcasvc HKLM\system\currentcontrolset\services\pcasvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\peerdistsvc Opens kev: Opens key: HKLM\system\currentcontrolset\services\peerdistsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\perfhost HKLM\system\currentcontrolset\services\perfhost\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\pla HKLM\system\currentcontrolset\services\pla\triggerinfo Opens key: HKLM\system\currentcontrolset\services\plugplay Opens kev: Opens key: HKLM\system\currentcontrolset\services\plugplay\triggerinfo Opens key: HKLM\system\currentcontrolset\services\pnrpautoreg Opens key: HKLM\system\currentcontrolset\services\pnrpautoreg\triggerinfo 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 Opens key: Opens key: HKLM\system\currentcontrolset\services\power Opens key: HKLM\system\currentcontrolset\services\power\triggerinfo HKLM\system\currentcontrolset\services\profsvc Opens key: Opens key: HKLM\system\currentcontrolset\services\profsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\protectedstorage HKLM\system\currentcontrolset\services\protectedstorage\triggerinfo Opens key: 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 Opens key: HKLM\system\currentcontrolset\services\remoteregistry Opens key: HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo HKLM\system\currentcontrolset\services\rpceptmapper Opens kev: Opens key: HKLM\system\currentcontrolset\services\rpceptmapper\triggerinfo Opens key: HKLM\system\currentcontrolset\services\rpclocator Opens key: HKLM\system\currentcontrolset\services\rpclocator\triggerinfo Opens key: HKLM\system\currentcontrolset\services\rpcss Opens key: HKLM\system\currentcontrolset\services\rpcss\triggerinfo Opens kev: HKLM\system\currentcontrolset\services\samss Opens key: HKLM\system\currentcontrolset\services\samss\triggerinfo HKLM\system\currentcontrolset\services\scardsvr Opens key: HKLM\system\currentcontrolset\services\scardsvr\triggerinfo Opens key: ${\tt HKLM \backslash system \backslash current control set \backslash services \backslash schedule}$ Opens key: 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 HKLM\system\currentcontrolset\services\seclogon Opens key: Opens key: HKLM\system\currentcontrolset\services\seclogon\triggerinfo Opens key: HKLM\system\currentcontrolset\services\sens Opens key: ${\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ sens \verb|\ trigger info$ Opens key: HKLM\system\currentcontrolset\services\sensrsvc Opens key: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo $\label{lem:lem:ham} $$HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0$$ Opens key: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1 Opens key: Opens key: HKLM\system\currentcontrolset\services\sessionenv

Opens key: HKLM\system\currentcontrolset\services\sessionenv\triggerinfo Opens key: HKLM\system\currentcontrolset\services\shellhwdetection HKLM\system\currentcontrolset\services\shellhwdetection\triggerinfo Opens kev: ${\it HKLM \ } system \verb|\currentcontrolset \ | services \verb|\smptrap| }$ Opens key: Opens key: HKLM\system\currentcontrolset\services\snmptrap\triggerinfo Opens key: HKLM\system\currentcontrolset\services\spooler Opens key:

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

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

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

HKLM\system\currentcontrolset\services\sppuinotify\triggerinfo Opens key: HKLM\system\currentcontrolset\services\ssdpsrv Opens key: HKLM\system\currentcontrolset\services\ssdpsrv\triggerinfo Opens kev: Opens key: HKLM\system\currentcontrolset\services\sstpsvc Opens kev: HKLM\system\currentcontrolset\services\sstpsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\stisvc HKLM\system\currentcontrolset\services\stisvc\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\storsvc Opens key: HKLM\system\currentcontrolset\services\storsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0 Opens key: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\1 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
Onens key: HKLM\system\currentcontrolset\services\tabletinputservice\

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

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

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

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

Opens key: HKLM\system\currentcontrolset\service\termservice\triggerinfo

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

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

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

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

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

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

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 key: HKLM\system\currentcontrolset\services\ui0detect\triggerinfo

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

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

Opens key: ${\tt HKLM \ } {\tt System \ } {\tt current control set \ } {\tt services \ } {\tt upnphost}$

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

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

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

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

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

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
Opens key: HKLM\system\currentcontrolset\services\w32time\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\w32time\triggerinfo\2

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

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

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

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

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

Opens key: HKLM\system\currentcontrolset\services\wcncsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wcspluginservice

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

 $Opens \; key: \\ \qquad \qquad \text{HKLM} \\ \text{system} \\ \text{current control set} \\ \text{services} \\ \text{wdiservice host} \\$

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

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

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

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

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

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

Opens key: HKLM\system\currentcontrolset\services\wecsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wercplsupport

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

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

Opens key: HKLM\system\currentcontrolset\services\wersvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\wersvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\winhttpautoproxysvc

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

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

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

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

```
Opens key:
                                                                    HKLM\system\currentcontrolset\services\winrm\triggerinfo
     Opens key:
                                                                    HKLM\system\currentcontrolset\services\wlansvc
     Opens kev:
                                                                    HKLM\system\currentcontrolset\services\wlansvc\triggerinfo
     Opens key:
                                                                    HKLM\system\currentcontrolset\services\wmiapsrv
     Opens key:
                                                                    HKLM\system\currentcontrolset\services\wmiapsrv\triggerinfo
     Opens key:
                                                                    HKLM\system\currentcontrolset\services\wmpnetworksvc
     Opens key:
                                                                    HKLM\system\currentcontrolset\services\wmpnetworksvc\triggerinfo
                                                                    HKLM\system\currentcontrolset\services\wpcsvc
     Opens key:
     Opens key:
                                                                    HKLM\system\currentcontrolset\services\wpcsvc\triggerinfo
     Opens key:
                                                                    HKLM\system\currentcontrolset\services\wpdbusenum
                                                                    HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo
     Opens key:
     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 kev:
     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 kev:
     Opens key:
                                                                    HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\1
     Opens key:
                                                                    HKLM\system\currentcontrolset\services\wwansvc
     Opens key:
                                                                    HKLM\system\currentcontrolset\services\wwansvc\triggerinfo
     Opens key:
                                                                    \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\advanced}} \\
     Opens key:
                                                                    HKLM\software\microsoft\windows\currentversion\explorer\advanced
                                                                    Opens key:
     Opens key:
                                                                    HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
     Opens key:
                                                                    HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\treatas
     Opens key:
                                                                    HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\treatas
     Opens key:
                                                                    HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\progid
     Opens key:
                                                                    HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\progid
     Opens key:
                                                                    HKCU\software\classes\wow6432node\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}
     Opens key:
                                                                    HKCR\wow6432node\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
     Opens key:
                                                                    HKCU\software\classes\wow6432node\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\progid
                                                                    HKCR\wow6432node\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\progid
     Opens key:
                                                                    HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
     Opens kev:
355b7f55341b}\inprocserver32
                                                                    HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32
     Opens kev:
     Opens key:
                                                                    HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\inprochandler32
     Opens key:
                                                                    HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler32
                                                                    HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
     Opens kev:
355b7f55341b}\inprochandler
                                                                    HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler
     Opens key:
                                                                    HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}
     Opens key:
                                                                    HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}
     Opens key:
     Opens key:
                                                                    HKCU \setminus software \setminus classes \setminus clsid \setminus \{a2a9545d - a0c2 - 42b4 - 9708 - a0c2 - 42b4 - a0c2 - 42b4 - a0c2 - 42b4 - a0c2 - 42b4 - a0c2 - a
a0b2badd77c8}\treatas
                                                                    HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\treatas
     Opens key:
                                                                    HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-
     Opens key:
a0b2badd77c8}\progid
                                                                    HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\progid
     Opens key:
     Opens key:
                                                                    HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{a2a9545d-a0c2-42b4-9708-a2a9545d-a0c2-42b4-9708-a2a9545d-a0c2-42b4-9708-a2a9545d-a0c2-42b4-9708-a2a9545d-a0c2-42b4-9708-a2a9545d-a0c2-42b4-9708-a2a9545d-a0c2-42b4-9708-a2a9545d-a0c2-42b4-9708-a2a9545d-a0c2-42b4-9708-a2a9545d-a0c2-42b4-9708-a2a9545d-a0c2-42b4-9708-a2a9545d-a0c2-42b4-9708-a2a9545d-a0c2-42b4-9708-a2a9545d-a0c2-42b4-9708-a2a9545d-a0c2-42b4-9708-a2a9545d-a0c2-42b4-9708-a2a9545d-a0c2-42b4-9708-a2a9545d-a0c2-42b4-9708-a2a9545d-a0c2-42b4-9708-a2a9545d-a0c2-42b4-9708-a2a9545d-a0c2-42b4-9708-a2a9545d-a0c2-42b4-9708-a2a9545d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-9708-a2a954d-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-a0c2-42b4-
a0b2badd77c8}
                                                                    HKCR \setminus wow6432 \\ node \setminus clsid \setminus \{a2a9545\\ d-a0c2-42b4-9708-a0b2\\ badd77c8\}
     Opens key:
     Opens key:
                                                                    HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{a2a9545d - a0c2 - 42b4 - 9708 - a0c2 - 42b4 - a0c2 - 42b4 - a0c2 - 42b4 - a0c2 - 42b4 - a0c2 - a0c2
a0b2badd77c8}\progid
                                                                    HKCR \setminus wow6432 \\ node \setminus clsid \setminus \{a2a9545d-a0c2-42b4-9708-a0b2badd77c8\} \setminus progid
     Opens key:
     Opens key:
                                                                    HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-
 a0b2badd77c8}\inprocserver32
                                                                    HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprocserver32
     Opens key:
     Opens key:
                                                                    HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprochandler32
                                                                    HKCR \ clsid \ \{a2a9545d-a0c2-42b4-9708-a0b2badd77c8\} \ inprochandler 32
     Opens key:
     Opens key:
                                                                    HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-
 a0b2badd77c8}\inprochandler
                                                                    HKCR \ clsid \ \{a2a9545d-a0c2-42b4-9708-a0b2badd77c8\} \ \ in prochandler
     Opens key:
     Opens key:
                                                                    HKCU \setminus software \setminus classes \setminus clsid \setminus \{90aa3a4e-1cba-4233-b8bb-535773d48449\}
                                                                    HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}
     Opens kev:
     Opens key:
                                                                    HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-
 535773d48449}\treatas
     Opens key:
                                                                    HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\treatas
                                                                    HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-
     Opens key:
 535773d48449}\progid
                                                                    HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\progid
     Opens key:
     Opens key:
                                                                    HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{90 \\ aa \\ 3a \\ 4e - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb - 1 \\ cba - 4233 - b8 \\ bb
```

535773d48449}

HKCR\wow6432node\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449} Opens kev: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{90aa3a4e-1cba-4233-b8bb-4235-b8bb-4235-b8bb-4235-b8bb-4235-b8bb-4235-b8bb-425-b8bb$ Opens key:

535773d48449}\progid

Opens key: HKCR\wow6432node\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\progid

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

535773d48449}\inprocserver32

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

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

535773d48449}\inprochandler32

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

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

535773d48449}\inprochandler

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

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

Opens key: HKCR\applications\calc.exe

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

Opens key: HKU\s-1-5-20

Opens key: Opens key: $HKU \ s-1-5-20 \ software \ microsoft \ windows \ current version \ explorer \ user$

shell folders

Opens key: HKU\s-1-5-20\environment

HKU\s-1-5-20\volatile environment Opens kev: Opens key: HKU\s-1-5-20\volatile environment\0

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

options\sppsvc.exe

Opens key: HKLM\system\currentcontrolset\control\session manager\quota system\s-1-

5-20

Opens key: HKU\s-1-5-20\software\microsoft\windows nt\currentversion

Opens key: HKU\s-1-5-20\software\microsoft\windows

nt\currentversion\appcompatflags\layers

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\sppsvc.exe

Opens key: HKLM\system\currentcontrolset\control\mui\settings

Opens key: HKLM\software\microsoft\ole Opens key: HKCU\software\classes\ HKLM\software\classes Opens key: Opens key: HKCR\appid\sppsvc.exe

Opens key: HKLM\system\currentcontrolset\control\computername

Opens key: HKLM\software\microsoft\rpc\extensions

Opens key: HKLM\software\microsoft\cryptography\defaults\provider types\type 001 Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong

cryptographic provider

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

options\wmpnetwk.exe

HKLM\software\microsoft\windows Opens key: nt\currentversion\appcompatflags\custom\wmpnetwk.exe HKLM\software\microsoft\oleaut Opens kev:

HKLM\software\microsoft\windows media player nss\3.0 Opens key:

Opens key: HKCR\appid\wmpnetwk.exe

Opens key: HKLM\software\microsoft\windows\windows error reporting\wmr

Opens key: HKLM\software\policies\microsoft\windowsmediaplayer

Opens key: HKLM\software\microsoft\windows media player nss\3.0\udnrenderers HKLM\software\microsoft\windows media player nss\3.0\devices Opens kev: Opens key: HKLM\software\microsoft\windows media player nss\3.0\servers Opens key:

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

HKLM\software\microsoft\windows media foundation\platform Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\msasn1

Opens key: HKLM\software\wow6432node\microsoft\drm

Opens key: HKLM\software\microsoft\windows

nt\currentversion\softwareprotectionplatform

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

Opens key: $HKLM \verb|\software\m| icrosoft \verb|\cryptography\oid\encodingtype 0|$ Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype

0\cryptdlldecodeobjectex

 $HKLM \ \ \ \ 1$ Opens key: Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype

1\cryptdlldecodeobjectex

 ${\tt HKLM \setminus software \setminus microsoft \setminus cryptography \setminus oid \setminus encoding type}$ Opens key:

1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.1.1

Opens kev: HKLM\software\microsoft\cryptography\oid\encodingtype

1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.1

Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype

1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.11

Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype

1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.12

 ${\tt HKLM \setminus software \setminus microsoft \setminus cryptography \setminus oid \setminus encoding type}$ Opens kev:

1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.2

Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype

1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.3

Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.4 Opens key: HKLM\software\microsoft\windows media player nss\3.0\mac access control Opens key: HKLM\software\microsoft\windows media player nss\3.0\devices\00-00-00-00-00-00 Opens key: HKLM\software\microsoft\windows media player nss\3.0\devices\08-00-27e8-14-9e Opens kev: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091} Opens key: $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ 'f1b32785-6fba-4fcf-1000' and the software \ 'microsoft \ 'windows \ 'current version' and the software \ 'microsoft \ 'windows \ 'current version' and the software \ 'microsoft \ 'windows \ 'current version' and the software \ 'microsoft \ 'windows \ 'current \ 'windows \ 'current \ 'windows \ 'current \ 'windows \ 'w$ 9d55-7b8e7f157091}\propertybag Opens key: HKCU\software\microsoft\windows\currentversion\explorer Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\0 Opens kev: HKCU\control panel\international Opens key: HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings HKLM\software\microsoft\windows media player nss\3.0\server settings Opens key: Opens key: HKLM\software\microsoft\com3 HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02} Opens key: HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}\treatas Opens key: Opens key: HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}\progid Opens key: $HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}\\\\inprocserver32$ Opens key: $HKCR \verb|\clsid|{e2085f28-feb7-404a-b8e7-e659bdeaaa02} \verb|\inprochandler32| \\$ Opens key: $HKCR \verb|\clsid|{e2085f28-feb7-404a-b8e7-e659bdeaaa02} \verb|\inprochandler| \\$ Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\com\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84} Opens key: HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84} Opens key: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84} HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-Opens key: 323e85a1ce84}\treatas Opens key: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\treatas HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-Opens key: 323e85a1ce84}\progid HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\progid Opens kev: Opens key: HKCU\software\classes\wow6432node\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84} HKCR\wow6432node\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\progid HKCR\wow6432node\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\progid Opens kev: Opens key: 323e85a1ce84}\inprocserver32 HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprocserver32 Opens key: Opens key: HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprochandler32 HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprochandler32 Opens kev: Opens key: HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprochandler Opens key: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprochandler Opens key: HKLM\software\microsoft\security center Opens key: HKLM\software\policies\microsoft\internet explorer\security Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\0 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\1 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\2 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\3 $\label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ Opens key: settings\zones\4 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\0 Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}$ settings\zones\1 Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}$ settings\zones\2 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\3 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\4 Opens key: HKCU\software\policies\microsoft\internet explorer HKCU\software\microsoft\internet explorer\security Opens kev:

Opens key: HKCR\interface\{00000134-0000-0000-c000-00000000046} Opens key: HKCR\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\zones HKLM\software\microsoft\windows\currentversion\action Opens key:

HKLM\software\microsoft\internet explorer\security

center\providers\com\{ca236752-2e77-4386-b63b-0e34774a413d}

Opens key:

```
\label{locality} HKCU \setminus software \\ \\ classes \\ \\ clsid \\ \\ \{ca236752-2e77-4386-b63b-0e34774a413d\} \\ \\ \\ equivalent \\ \\ equiv
     Opens key:
     Opens key:
                                                                            HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}
                                                                            Opens key:
0e34774a413d}\treatas
     Opens kev:
                                                                            HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\treatas
     Opens key:
                                                                            HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\progid
                                                                            HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\progid
     Opens key:
     Opens key:
                                                                            HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{ca236752 - 2e77 - 4386 - b63b 
0e34774a413d}
     Opens key:
                                                                            HKCR\wow6432node\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}
     Opens key:
                                                                            HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\inprocserver32
                                                                           HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprocserver32
     Opens key:
     Opens key:
                                                                            HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\inprochandler32
     Opens key:
                                                                           HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprochandler32
     Opens key:
                                                                            HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\inprochandler
                                                                          HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprochandler
     Opens key:
     Opens key:
                                                                            HKLM\software\microsoft\wbem\cimom
     Opens key:
                                                                            HKLM\software\policies\microsoft\windows\windows error reporting
                                                                            HKLM\software\microsoft\windows\windows error reporting
     Opens kev:
     Opens key:
                                                                            HKCU\software\policies\microsoft\windows\windows error reporting
     Opens key:
                                                                            HKCU\software\microsoft\windows\windows error reporting
     Opens key:
                                                                            HKCU\software\microsoft\windows\windows error reporting\erc
     Opens key:
                                                                            HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}
     Opens key:
                                                                            HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}
                                                                            HKCU \setminus software \setminus classes \setminus clsid \setminus \{88d96a05 - f192 - 11d4 - a65f - f192 - f
     Opens kev:
0040963251e5}\treatas
     Opens key:
                                                                            HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\treatas
                                                                            HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-
     Opens key:
0040963251e5}\progid
     Opens key:
                                                                            HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\progid
                                                                           HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-
     Opens key:
0040963251e5}\inprocserver32
     Opens key:
                                                                           HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprocserver32
                                                                           HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-
     Opens key:
0040963251e5}\inprochandler32
     Opens key:
                                                                           HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprochandler32
     Opens key:
                                                                           HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-
0040963251e5}\inprochandler
     Opens key:
                                                                           HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprochandler
                                                                            HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}
     Opens key:
     Opens key:
                                                                            HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}\proxystubclsid32
     Opens key:
                                                                            HKLM\software\microsoft\msxml60
                                                                           Opens key:
980053277-1733835069-2361817685-1001
                                                                           HKCR\clsid\{00020424-0000-0000-c000-00000000046}
     Opens kev:
                                                                            HKCR\clsid\{00020424-0000-0000-c000-00000000046}\treatas
     Opens key:
     Opens key:
                                                                            HKCR\clsid\{00020424-0000-0000-c000-00000000046}\progid
     Opens key:
                                                                            HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}
                                                                            \label{local-cond} \mbox{HKCR} $$ Wow6432 node\clsid\\ 00020424-0000-0000-c000-00000000046\\ \mbox{progid} $$ $$ \mbox{HKCR}$$ $$ Wow6432 node\clsid\\ \mbox{progid} $$ \mbox{progid} $$ \mbox{progid} $$ \mbox{progid} $$ $$ \mbox{progid} $$ \mbox{pr
     Opens key:
     Opens key:
                                                                            Opens kev:
                                                                            HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprochandler32
                                                                            Opens key:
     Opens key:
                                                                            Opens key:
                                                                            HKCR\wow6432node\interface\{adda3d55-6f72-4319-bff9-
18600a539b10}\forward
     Opens key:
                                                                            HKCR\interface {adda3d55-6f72-4319-bff9-18600a539b10} \land typelib
     Opens key:
                                                                            HKCR\typelib\{db3442a7-a2e9-4a59-9cb5-f5c1a5d901e5}
                                                                            HKCR\typelib\{db3442a7-a2e9-4a59-9cb5-f5c1a5d901e5}\1.0
     Opens key:
     Opens key:
                                                                            {\it HKLM} \verb|\software\microsoft\windows\currentversion\action
center\providers\com\{c8e6f269-b90a-4053-a3be-499afcec98c4}
                                                                            HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}
     Opens key:
     Opens key:
                                                                            HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}
     Opens key:
                                                                            HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-
```

499afcec98c4}\treatas

Opens key: HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\treatas HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-Opens kev:

499afcec98c4}\progid

Opens key: HKCR\typelib\{db3442a7-a2e9-4a59-9cb5-f5c1a5d901e5}\1.0\0 Opens key: HKCR\typelib\{db3442a7-a2e9-4a59-9cb5-f5c1a5d901e5}\1.0\0\win64 HKCR\typelib\{db3442a7-a2e9-4a59-9cb5-f5c1a5d901e5}\1.0\0\win32 Opens key: Opens key: HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\progid Opens key: HKCU\software\classes\wow6432node\clsid\{c8e6f269-b90a-4053-a3be-

499afcec98c4}

 $HKCR \ wow 6432 node \ clsid \ \{c8e6f269-b90a-4053-a3be-499afcec98c4\}$ Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{c8e6f269-b90a-4053-a3be-

499afcec98c4}\progid

Opens key: $HKCR \setminus wow6432 node \\ clsid \\ \{c8e6f269-b90a-4053-a3be-499afcec98c4\} \setminus progide \\ (c8e6f269-b90a-4053-a3be-499afcec98c4) \\ (c8e6f269-b90a-4053-a3be-499afcec98c$

HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-Opens key:

499afcec98c4}\inprocserver32

```
HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\
      Opens key:
      Opens key:
                                                                                   HKCR\typelib
                                                                                   HKCR\typelib\{00020430-0000-0000-c000-00000000046}
      Opens kev:
      Opens key:
                                                                                   HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0
      Opens key:
                                                                                   HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0
      Opens key:
                                                                                   \label{limit} $HKCR \times 00020430-0000-0000-c000-00000000046} \ \ 2.0 \times 0.0 \times 0
                                                                                   HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-
      Opens key:
499afcec98c4}\inprochandler32
                                                                                   HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\\\\
      Opens key:
                                                                                   HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-
      Opens key:
499afcec98c4}\inprochandler
      Opens key:
                                                                                   HKCR \ clsid \ \{c8e6f269-b90a-4053-a3be-499afcec98c4\} \ in prochandler
      Opens key:
Opens key:
                                                                                   HKLM\software\microsoft\windows\currentversion\policies\system
                                                                                   HKCR\interface\{00020400-0000-0000-c000-00000000046}
      Opens key:
                                                                                   HKCR\interface\{00020400-0000-0000-0000-00000000046}\proxystubclsid32
      Opens kev:
      Opens key:
                                                                                   HKCR\clsid\{00020420-0000-0000-c000-00000000046}
      Opens key:
                                                                                   HKCR\clsid\{00020420-0000-0000-c000-000000000046}\treatas
      Opens key:
                                                                                   HKCR\clsid\{00020420-0000-0000-c000-00000000046}\progid
      Opens key:
                                                                                   HKLM\software\microsoft\windows\currentversion\action
 center\providers\com\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
                                                                                   HKCU\software\classes\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
      Opens kev:
      Opens key:
                                                                                   HKCR\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
      Opens key:
                                                                                   5017a56357c3}
      Opens key:
                                                                                   HKCR\wow6432node\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
      Opens key:
                                                                                   HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}
      Opens key:
                                                                                   HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}
      Opens key:
                                                                                   HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-
40cd513679d5}\treatas
                                                                                   HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\treatas
      Opens key:
      Opens key:
                                                                                   HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-
40cd513679d5}\progid
                                                                                   HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\progid
      Opens key:
      Opens key:
                                                                                   HKCU\software\classes\wow6432node\clsid\{900c0763-5cad-4a34-bc1f-
40cd513679d5}
                                                                                   HKCR\wow6432node\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}
      Opens key:
      Opens key:
                                                                                   HKCU\software\classes\wow6432node\clsid\{900c0763-5cad-4a34-bc1f-
40cd513679d5}\progid
                                                                                   HKCR\wow6432 node\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\\progid
      Opens key:
      Opens key:
                                                                                   HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}
      Opens key:
                                                                                   HKCR\wow6432node\clsid\{00020420-0000-0000-c000-00000000046}\progid
                                                                                   \label{local-cond} \verb+KCR\clsid+\{00020420-0000-0000-c000-000000000046\}+ in procserver 32, and the second statement of the sec
      Opens key:
      Opens key:
                                                                                   HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprochandler32
      Opens key:
                                                                                   HKLM\software\microsoft\windows\currentversion\action
 center\providers\eventlog\{01979c6a-42fa-414c-b8aa-eee2c8202018}
      Opens key:
                                                                                   HKCR\interface\{e3bf6178-694e-459f-a5a6-191ea0ffa1c7}
      Opens kev:
                                                                                   Opens key:
      Opens key:
                                                                                   HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-
40cd513679d5}\inprocserver32
                                                                                   HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\ inprocserver32
      Opens key:
                                                                                   HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-
      Opens key:
40cd513679d5}\inprochandler32
                                                                                   \label{lem:hkcr} $$ HKCR\clsid_{900c0763-5cad-4a34-bc1f-40cd513679d5} \in \clsid_{900c0763-5cad-4a34-bc1f-40cd513679d5} $$ inprochandler 32 $$ in the context of the contex
      Opens key:
                                                                                   HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-
      Opens key:
40cd513679d5}\inprochandler
                                                                                   HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\ inprochandler
      Opens key:
      Opens key:
                                                                                   HKCU \setminus software \setminus classes \setminus interface \setminus \{b722bccb-4e68-101b-a2bc-00aa00404770\}
      Opens key:
                                                                                   Opens key:
                                                                                   191eaOffa1c7}\forward
      Opens key:
                                                                                   HKCR\interface\{e3bf6178-694e-459f-a5a6-191ea0ffa1c7\}\typelib
                                                                                   HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}
      Opens key:
      Opens key:
                                                                                   HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc-
 00aa00404770}\proxystubclsid32
                                                                                  HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32
      Opens key:
      Opens key:
                                                                                   HKCU \setminus software \setminus classes \setminus clsid \setminus \{a4a1a128-768f-41e0-bf75-e4fddd701cba\}
      Opens key:
                                                                                   HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
      Opens key:
                                                                                   HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-
 e4fddd701cba}\treatas
                                                                                   HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\treatas
      Opens kev:
                                                                                   HKCU \setminus software \setminus classes \setminus clsid \setminus \{a4a1a128-768f-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e
      Opens key:
e4fddd701cba}\progid
      Opens key:
                                                                                   HKLM\software\microsoft\windows\currentversion\action
 center\providers\eventlog\{945a8954-c147-4acd-923f-40c45405a658}
                                                                                   HKCR\clsid\\a4a1a128-768f-41e0-bf75-e4fddd701cba\\progid
      Opens kev:
      Opens key:
                                                                                   e4fddd701cba}
      Opens key:
                                                                                   HKCR \setminus wow 6432 \\ node \\ clsid \\ \{a4a1a128-768f-41e0-bf75-e4fddd \\ 701cba\}
      Opens key:
                                                                                   HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{a4a1a128-768f-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-
e4fddd701cba}\progid
```

```
Opens key: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\progid Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32
```

Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32

Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-

e4fddd701cba}\inprochandler32

Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler32

Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-

e4fddd701cba}\inprochandler

Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler

Opens key: ${\tt HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus action}$

center\providers\eventlog\{dab69a6a-4d2a-4d44-94bf-e0091898c881}

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

 $center \verb|\providers| eventlog \verb|\fill 11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78| |$

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

options[disableusermodecallbackfilter]

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: HKLM\system\currentcontrolset\control\nls\customlocale[empty]

Queries value:

HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]

Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]

Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-

us[alternatecodepage]

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

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [prefer external manifest]$

Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]

Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]

Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]

nt\currentversion\windows[loadappinit_dlls]

Queries value: HKLM\software\wow6432node\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\wow6432node\microsoft\windows\windows error

reporting\wmr[disable]

Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]

Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options[disablelocaloverride]

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

options\dllnxoptions[untfs.dll]

. Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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:

Queries value:

| MKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000003[packedcatalogitem] |
| Oueries value:

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

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries \ 0000000000007 \ [packed catalog item] \\ Queries \ value:$

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem] Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
 Oueries 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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
 Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 0000000000001 \ [enabled] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version] Oueries value:
- $HKLM \system \current control set \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000002[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
 Queries value:
- $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \namespace_catal$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[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\000000000003[librarypath]
- 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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
 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\00000000004[librarypath]
 Queries 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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace]
 Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace_catalog5 \catalog_entries \0000000000004 \cite{lemabled} \end{subarray} Queries value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
 Oueries value:

Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace_catalog \le catalog_entries \setminus 0000000000005 [displaystring]$

Queries value:

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

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

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

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

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\000000000006[providerid]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
Queries 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\000000000006[enabled]
Queries 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]

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

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]

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

Queries value:

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

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:

Queries value:

Queries value:

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

Queries value:

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

VIM) seftware)

Queries value:

 $\label{lem:hklmlsoftware} HKLM\software\wow6432 node\microsoft\cryptography\defaults\provider\microsoft\ base\ cryptographic\provider\v1.0[image\path]$

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

manager[safeprocesssearchmode]

Queries value: HKLM\system\currentcontrol\sa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrol\sat{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\rpc[maxrpcsize]

Queries value:

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

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

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

Queries value: <LM\system\ci</pre>
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010[packedcatalogitem]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009[packedcatalogitem] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008[packedcatalogitem]
 Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007[packedcatalogitem]
 Oueries value:

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005[packedcatalogitem]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004[packedcatalogitem]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000003[packedcatalogitem]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002[packedcatalogitem] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001[packedcatalogitem]
 Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [current_namespace_catalog]$

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[providerid]

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[providerid] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[providerid]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[providerid]

Oueries value:

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\software\microsoft\windows

nt\currentversion\profilelist[programdata]

Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[public] Oueries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[default] Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir] Queries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir] $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version [program files dir (x86)] \\$ Oueries value: Queries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir (x86)] Queries value: HKLM\software\microsoft\windows\currentversion[programw6432dir] Oueries value: HKLM\software\microsoft\windows\currentversion[commonw6432dir] $HKLM \ \ \, in the constraint of the constrai$ Queries value:

18[profileimagepath]

 $\label{thm:linear} Queries \ value: \\ HKU\.default\software\mbox{\sc microsoft\windows\currentversion\explorer\user}$

shell folders[appdata]

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

shell folders[local appdata]

Queries value:

HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
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\software\microsoft\windows

nt\currentversion\windows[loadappinit_dlls]

 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:

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

Oueries value: Queries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[type] Queries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[guid] Queries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[datatype0] HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[action] Oueries value: Oueries 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] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[action] Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[type] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[guid] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype0] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data0] Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype1] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data1] Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype2]

Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data2] HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype3] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[action] Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[type] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[guid] Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype0] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data0] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype1] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data1] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype2] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data2] Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype3] Oueries value: HKLM\system\currentcontrolset\services\browser[imagepath] HKLM\system\currentcontrolset\services\browser[type] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\browser[start] Oueries value: HKLM\system\currentcontrolset\services\browser[errorcontrol] Queries value: HKLM\system\currentcontrolset\services\browser[tag] Queries 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] Queries value: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[action] Queries value: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[type] $HKLM \verb|\system| current controlset \verb|\services| bthserv \verb|\triggerinfo| 0 [guid]$ Queries value: Oueries value: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[datatype0] Oueries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[action] Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[type] Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[guid] HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[datatype0] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[data0] Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[datatype1] Oueries value: HKLM\system\currentcontrolset\services\dnscache[imagepath] HKLM\system\currentcontrolset\services\dnscache[type] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache[start] Oueries value: HKLM\system\currentcontrolset\services\dnscache[errorcontrol] HKLM\system\currentcontrolset\services\dnscache[tag] Queries value: Queries value: HKLM\svstem\currentcontrolset\services\dnscache[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\dnscache[dependongroup] HKLM\system\currentcontrolset\services\dnscache[group] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache[objectname] $HKLM \verb|\system| current controlset \verb|\services| efs \verb|\triggerinfo| 0 [action]$ Oueries value: Queries value: HKLM\system\currentcontrolset\services\efs\triggerinfo\0[type] Oueries value: HKLM\svstem\currentcontrolset\services\efs\triggerinfo\0[guid] Oueries value: HKLM\system\currentcontrolset\services\efs\triggerinfo\0[datatype0] Oueries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[action] Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[type] Oueries value: Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[datatype0] HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[data0] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[datatype1] Oueries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[action] Oueries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[type] Oueries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[guid] Queries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[datatype0] Oueries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[data0] Queries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[datatype1] Oueries value: HKLM\system\currentcontrolset\services\ikeext[imagepath] Oueries value: HKLM\system\currentcontrolset\services\ikeext[type] Oueries value: HKLM\system\currentcontrolset\services\ikeext[start] HKLM\system\currentcontrolset\services\ikeext[errorcontrol] Queries value: Queries value: HKLM\system\currentcontrolset\services\ikeext[tag] Oueries value: HKLM\system\currentcontrolset\services\ikeext[dependonservice] Queries value: HKLM\system\currentcontrolset\services\ikeext[dependongroup] Queries value: HKLM\system\currentcontrolset\services\ikeext[group] Oueries value: HKLM\system\currentcontrolset\services\ikeext[objectname] Oueries value: Queries value: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[type] Oueries value: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[guid] Queries value: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[datatype0] Oueries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[action] Oueries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[type] Oueries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[guid] Oueries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[datatype0] Oueries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[action] Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[type] HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[guid] Oueries value: Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[datatype0] Oueries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a66e19e6] Oueries value: HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]

Queries value:

HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]

Queries value: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[action]

```
Oueries value:
                         HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[type]
                         HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[guid]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype0]
                         HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[data0]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype1]
                         HKLM\system\currentcontrolset\services\policyagent[imagepath]
 Oueries value:
 Oueries value:
                         HKLM\system\currentcontrolset\services\policyagent[type]
                         HKLM\system\currentcontrolset\services\policyagent[start]
 Oueries value:
 Oueries value:
                         HKLM\system\currentcontrolset\services\policyagent[errorcontrol]
 Queries value:
                         HKLM\system\currentcontrolset\services\policyagent[tag]
 Oueries value:
                         HKLM\system\currentcontrolset\services\policyagent[dependonservice]
 Oueries value:
                         HKLM\system\currentcontrolset\services\policyagent[dependongroup]
 Oueries value:
                         HKLM\system\currentcontrolset\services\policyagent[group]
 Oueries value:
                         HKLM\system\currentcontrolset\services\policyagent[objectname]
                         HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[action]
 Oueries value:
 Queries 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]
 Queries value:
                         HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[type]
                         HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[guid]
 Oueries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[datatype0]
 Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[action]
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[type]
 Oueries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[guid]
 Oueries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data0]
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data1]
HKLM \setminus system \setminus current control set \setminus services \setminus table tinput service \setminus trigger in fo \setminus 0 \ [data type 2]
 Oueries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data2]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus table tinput service \setminus trigger info \setminus 0 [data type 3]
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data3]
 Oueries value:
Oueries value:
                         HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[action]
 Oueries value:
                         HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[type]
                         HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[guid]
 Oueries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[datatype0]
 Oueries value:
                         HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[action]
 Queries value:
                         HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[type]
 Oueries value:
                         HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[guid]
 Queries value:
                         HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[datatype0]
 Oueries value:
                         HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[action]
 Oueries value:
                         HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[type]
 Oueries value:
                         HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[guid]
 Queries value:
HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[datatype0]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[action]
                         HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[type]
 Queries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[guid]
                         HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[datatype0]
 Oueries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[action]
 Queries value:
                         HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[type]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[guid]
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[datatype0]
                         HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[action]
 Queries value:
                         HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[type]
 Oueries value:
 Oueries value:
                         HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[guid]
 Oueries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[datatype0]
                         HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[action]
 Oueries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[type]
                         HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[guid]
 Oueries value:
 Oueries value:
```

HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[datatype0]

HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[action]
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[type]

HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[guid]

Queries value:

Queries value: Queries value:

Oueries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[datatype0] HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[action] Oueries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[type] Queries value: Oueries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[guid] Queries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype0] Queries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[data0] Oueries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype1] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[typeahead] Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\advanced[typeahead] HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}[] HKCR\clsid\{660b90c8-73a9-4b58-8cae-Oueries value: 355b7f55341b}\inprocserver32[inprocserver32] HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32[] Oueries value: HKCR\clsid\{660b90c8-73a9-4b58-8cae-Queries value: 355b7f55341b}\inprocserver32[threadingmodel] Oueries value: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}[] HKCR\clsid\{a2a9545d-a0c2-42b4-9708-Oueries value: a0b2badd77c8}\inprocserver32[inprocserver32] HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprocserver32[] Queries value: Oueries value: HKCR\clsid\{a2a9545d-a0c2-42b4-9708a0b2badd77c8}\inprocserver32[threadingmodel] Oueries value: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}[] HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-Oueries value: 535773d48449}\inprocserver32[inprocserver32] Queries value: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprocserver32[] HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-Oueries value: 535773d48449}\inprocserver32[threadingmodel] Queries value: HKLM\system\currentcontrolset\services\dcomlaunch[objectname] Oueries value: HKLM\system\currentcontrolset\services\rpceptmapper[objectname] Queries value: HKLM\system\currentcontrolset\services\rpcss[objectname] Queries value: HKLM\system\currentcontrolset\services\eventsystem[objectname] Oueries value: HKLM\system\currentcontrolset\services\bits[objectname] Queries value: HKLM\system\currentcontrolset\services\bits[imagepath] Queries value: HKLM\system\currentcontrolset\services\bits[wow64] Oueries value: HKLM\system\currentcontrolset\services\bits[requiredprivileges] Queries value: HKLM\system\currentcontrolset\services\bits[type] Queries value: HKLM\system\currentcontrolset\services\bits[start] Oueries value: HKLM\system\currentcontrolset\services\bits[errorcontrol] Queries value: HKLM\system\currentcontrolset\services\bits[tag] Queries value: HKLM\system\currentcontrolset\services\bits[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\bits[dependongroup] Queries value: HKLM\system\currentcontrolset\services\bits[group] Queries value: HKLM\system\currentcontrolset\services\fontcache[objectname] Oueries value: HKLM\system\currentcontrolset\services\fontcache[imagepath] Queries value: HKLM\system\currentcontrolset\services\fontcache[wow64] Queries value: HKLM\system\currentcontrolset\services\fontcache[requiredprivileges] Oueries value: HKLM\system\currentcontrolset\services\http[objectname] Queries value: HKLM\system\currentcontrolset\services\ssdpsrv[objectname] Queries value: HKLM\system\currentcontrolset\services\ssdpsrv[imagepath] Oueries value: HKLM\system\currentcontrolset\services\ssdpsrv[wow64] Queries value: HKLM\system\currentcontrolset\services\ssdpsrv[requiredprivileges] Oueries value: HKLM\svstem\currentcontrolset\services\sppsvc[objectname] Queries value: HKLM\system\currentcontrolset\services\sppsvc[imagepath] HKLM\system\currentcontrolset\services\sppsvc[wow64] Oueries value: Queries value: HKLM\system\currentcontrolset\services\sppsvc[requiredprivileges] $HKLM \ \ \, in the constant of the constant$ Oueries value: 20[profileimagepath] Queries value: HKU\s-1-5-20\software\microsoft\windows\currentversion\explorer\user shell folders[appdata] Queries value: $HKU \ s-1-5-20 \ software \ microsoft \ windows \ current version \ explorer \ user$ shell folders[local appdata] HKLM\system\currentcontrolset\services\sppsvc[environment] Oueries value: Queries value: HKLM\system\currentcontrolset\control\mui\settings[preferreduilanguages] Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[sppsvc] Queries value: HKLM\system\currentcontrolset\control\wmi\security[bf3736e4-23ae-47c3b472-a03c2c3550fe] Queries value: HKLM\system\currentcontrolset\control\wmi\security[5b6189d4-c1fd-4a8c-9910-9b6fad873da7] Oueries value: HKLM\system\currentcontrolset\control\wmi\security[e23b33b0-c8c9-472ca5f9-f2bdfea0f1561 Queries value: $HKLM \setminus system \setminus current control \setminus lsa[everyone includes an onymous]$ Oueries value: HKLM\software\microsoft\rpc\extensions[remoterpcdll] Queries value: HKLM\software\microsoft\cryptography\defaults\provider types\type 001[name] Oueries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[type] Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong

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

cryptographic provider[image path]

Oueries value: HKLM\system\currentcontrolset\services\wmpnetworksvc[imagepath] Oueries value: HKLM\system\currentcontrolset\services\wmpnetworksvc[wow641

Oueries value: HKLM\system\currentcontrolset\services\wmpnetworksvc[requiredprivileges]

Queries value: HKLM\system\currentcontrolset\services\wmpnetworksvc[environment]

HKLM\software\microsoft\windows Oueries value:

nt\currentversion\compatibility32[wmpnetwk]

Queries value: HKLM\system\currentcontrolset\control\wmi\security[a7eb57f6-145e-4f18-

bd75-dbbf6f7e23a71

Queries value: HKLM\system\currentcontrolset\control\wmi\security[6a2dc7c1-930a-4fb5-

bb44-80b30aebed6c1

Oueries value: HKLM\software\microsoft\windows media player

nss\3.0[idlesecondsuntilsleep]

Queries value: HKLM\software\microsoft\windows media player

nss\3.0[idlesecondsuntilmemoryflush]

Queries value: HKLM\software\microsoft\windows media player

nss\3.0[secondstocachefirewallstatus]

HKLM\software\microsoft\windows media player nss\3.0[enabledlnatags] Oueries value: Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]

Queries value: HKLM\software\microsoft\windows\currentversion[devicepath]

Oueries value: HKLM\software\microsoft\windows media player

nss\3.0[upnppingintervaloverrideinseconds]

Queries value: HKLM\system\currentcontrolset\services\wuauserv[objectname] HKLM\svstem\currentcontrolset\services\wuauserv[imagepath] Oueries value: Queries value: HKLM\system\currentcontrolset\services\wuauserv[wow64]

Queries value:

HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]

HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity] Queries value: Queries value: HKLM\system\currentcontrolset\services\wuauserv[requiredprivileges] Oueries value: HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder] Queries value: HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]

Queries value: HKLM\software\microsoft\cryptography\rng[seed]

HKLM\software\microsoft\windows media foundation\platform[freewpptrace] Queries value:

 $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| drm[last sessionid]|$ Queries value:

Queries value:

b9b8-05e4eca4977e]

HKLM\system\currentcontrolset\control\wmi\security[0a592d4d-6d8e-403d-Queries value:

9a4a-4d5e94dc5dc5]

Oueries value:

b9b8-05e4eca4977e]

Queries value: HKLM\system\currentcontrolset\control\wmi\security[00000002-0dc9-401d-

b9b8-05e4eca4977e]

Queries value: HKLM\system\currentcontrolset\control\wmi\security[00000003-0dc9-401d-

b9b8-05e4eca4977e]

Queries value: b9b8-05e4eca4977e]

Queries value:

HKLM\system\currentcontrolset\control\wmi\security[00000005-0dc9-401db9b8-05e4eca4977e]

Queries value:

HKLM\system\currentcontrolset\control\wmi\security[00000006-0dc9-401d-

b9b8-05e4eca4977e]

Queries value: HKLM\system\currentcontrolset\services\crypt32[diaglevel] HKLM\system\currentcontrolset\services\crypt32[diagmatchanymask] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\cryptsvc[imagepath] Queries value: HKLM\system\currentcontrolset\services\cryptsvc[type] Queries value: HKLM\system\currentcontrolset\services\cryptsvc[start] Oueries value: HKLM\system\currentcontrolset\services\cryptsvc[errorcontrol] Queries value: HKLM\system\currentcontrolset\services\cryptsvc[tag]

Oueries value: HKLM\system\currentcontrolset\services\cryptsvc[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\cryptsvc[dependongroup] Oueries value: HKLM\system\currentcontrolset\services\cryptsvc[group] Queries value: HKLM\system\currentcontrolset\services\cryptsvc[objectname]

Queries value: HKLM\software\wow6432node\microsoft\drm[datapath] Oueries value: HKLM\software\wow6432node\microsoft\drm[upgradepath] $\label{locations} \verb|HKLM\| software \verb| microsoft\| ole[maximum allowed allocation size]| \\$ Queries value:

Oueries value: HKLM\software\microsoft\windows media player nss\3.0\devices[00-00-00-

00-00-001

HKLM\software\microsoft\windows media player nss\3.0\devices\00-00-00-Oueries value: 00-00-00[defaultauthorization]

 $HKLM \ software \ microsoft \ windows \ media \ player \ nss \ \ 3.0 \ devices \ [08-00-27-00]{\ devices} \ [08-00-27-00]{\ dev$

Queries value:

e8-14-9e1 Oueries value: HKLM\software\microsoft\windows media player nss\3.0\devices\08-00-27-

e8-14-9e[defaultauthorization]

9d55-7b8e7f157091}[category]

Queries value:

9d55-7b8e7f157091}[name]

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[parentfolder]

Queries value:

9d55-7b8e7f157091}[description]

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [relative path]$

Queries value:

 $\label{thm:local-operator} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\fifth{1}{5}2785-6fba-4fcf-9d55-7b8e7f157091\fifth{1}{5}parsing name\figure{1}{2}$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \find \find \current \find \current \find \current \cur$

Oueries value:

Oueries value:

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [security]$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [stream resource]$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[stream resource type]$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [local redirect only]$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[roamable]$

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ (f1b32785-6fba-4fcf-9d55-7b8e7f157091) \ [precreate]$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[stream]$

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [publish \ explorer\ \]$

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\fifth{1}{5}2785-6fba-4fcf-9d55-7b8e7f157091\fifth{1}{5}2785-7b8e7f157091\fifth{1}{5}2785-7b8e7f157091\fifth{1}{5}2785-7b8e7f157091\fifth{1}{5}2785-7b8e7f157091\fifth{1}{5}2785-7b8e7f157091\fifth{1}{5}2785-7b8e7f157091\fifth{1}{5}2785-7b8e7f157091\fifth{1}{5}2785-7b8e7f157091\fifth{1}{5}2785-7b8e7f157091\fifth{1}{5}2785-7b8e7f157091\fifth{1}{5}2785-7b8e7f157091\fifth{1}{5}2785-7b8e7f157091\fifth{1}{5}2$

Queries value:

Queries value:

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[local appdata]

Queries value: HKLM\software\microsoft\windows media player nss\3.0\devices\00-00-00-

00-00-00[alive]

Queries value: HKLM\software\microsoft\windows media player nss\3.0\devices\08-00-27-

e8-14-9e[alive]

Queries value: HKLM\software\microsoft\com3[com+enabled]

Queries value: HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}\progid[]
Queries value: HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}[]

Queries value: HKCR\clsid\{e2085f28-feb7-404a-b8e7-

e659bdeaaa02}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}\inprocserver32[]

Queries value: HKCR\clsid\{e2085f28-feb7-404a-b8e7-

e659bdeaaa02}\inprocserver32[threadingmodel]

Queries value: HKLM\software\microsoft\ole[maxsxshashcount]
Queries value: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}[]

Queries value: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-

323e85a1ce84}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprocserver32[]

Queries value: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-

323e85a1ce84}\inprocserver32[threadingmodel]

Queries value: HKLM\system\currentcontrolset\control\wmi\security[1b0ac240-cbb8-4d55-

8539-9230a44081a5]

Queries value: HKLM\system\currentcontrolset\control\wmi\security[5857d6ca-9732-4454-

809b-2a87b70881f8]

Queries value: HKLM\system\currentcontrolset\control\wmi\security[9dac2c1e-7c5c-40eb-

833b-323e85a1ce84]

Queries value: HKLM\software\policies\microsoft\internet

explorer\security[disablesecuritysettingscheck]

Queries value: HKLM\software\policies\microsoft\internet

explorer\security[disablefixsecuritysettings]
 Queries value: HKCU\software\microsoft\internet

explorer\security[disablefixsecuritysettings]
 Queries value: HKCR\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32[]

Queries value: HKCR\interface\{00000134-0000-00 Queries value: HKLM\software\microsoft\internet

```
HKCU\software\microsoft\windows\currentversion\action
  Oueries value:
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.106[checksetting]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.101[checksetting]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.103[checksetting]
                                    HKCU\software\microsoft\windows\currentversion\action
  Oueries value:
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.100[checksetting]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.102[checksetting]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.104[checksetting]
  Oueries value:
                                   HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Queries value:
                                    HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}[]
  Queries value:
                                    HKCR\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\inprocserver32\inprocserver321
                                    HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprocserver32[]
  Queries value:
  Oueries value:
                                    HKCR\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\inprocserver32[threadingmodel]
                                    HKLM\software\microsoft\wbem\cimom[logging]
  Queries value:
  Queries value:
                                    HKLM\system\currentcontrolset\control\wmi\security[a0ef609d-0a14-424c-
9270-3b2691a0a3941
  Queries value:
                                    HKLM\software\microsoft\sqmclient\windows\disabledprocesses[5512633]
  Queries value:
                                    HKLM\software\microsoft\com3[gipactivitybypass]
  Oueries value:
                                    HKLM\system\currentcontrolset\control\wmi\security[3e19a300-75d9-4027-
86ba-948b70416220]
  Queries value:
                                    HKLM\software\microsoft\windows\windows error reporting[disabled]
                                    HKCU\software\microsoft\windows\windows error reporting[disabled]
  Oueries value:
  Queries value:
                                    HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\progid[]
  Queries value:
                                    HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}[]
                                    HKCR\clsid\{88d96a05-f192-11d4-a65f-
  Queries value:
0040963251e5}\inprocserver32[inprocserver32]
  Queries value:
                                    HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprocserver32[]
                                    HKCR\clsid\{88d96a05-f192-11d4-a65f-
  Oueries value:
0040963251e5}\inprocserver32[threadingmodel]
                                    HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
  Oueries value:
980053277-1733835069-2361817685-1001[profileimagepath]
                                    HKCR \land (adda3d55-6f72-4319-bff9-18600a539b10) \land (adda3d55-6f72-4319-bff9-18600a55-6f72-4500a55-6f72-4500a55-6f72-4500a55-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f72-4500a5-6f7
  Queries value:
                                    HKCR\clsid\{00020424-0000-0000-c000-00000000046}[]
  Queries value:
                                    HKCR\clsid\{00020424-0000-0000-c000-
  Oueries value:
00000000046}\inprocserver32[inprocserver32]
                                    HKCU\software\microsoft\windows\currentversion\action
  Oueries value:
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.100[checksetting]
                                    HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprocserver32[]
  Oueries value:
                                    HKCR\clsid\{00020424-0000-0000-c000-
  Queries value:
00000000046}\inprocserver32[threadingmodel]
  Queries value:
                                    HKCU\software\microsoft\windows\windows error
reporting[lastqueuepestertime]
  Queries value:
                                    HKLM\software\microsoft\windows\windows error
reporting[queuepesterinterval]
                                    HKCU\software\microsoft\windows\windows error
  Oueries value:
reporting[queuepesterinterval]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\action
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2\}.check.101[checksetting]
  Queries value:
                                    HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}\typelib[]
                                    HKCR \land [adda3d55-6f72-4319-bff9-18600a539b10] \land [version]
  Queries value:
                                    HKCR\typelib\{db3442a7-a2e9-4a59-9cb5-f5c1a5d901e5}\1.0\0\win32[]
  Oueries value:
                                    HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}[]
  Oueries value:
                                    HKCR\clsid\{c8e6f269-b90a-4053-a3be-
499afcec98c4}\inprocserver32[inprocserver32]
  Oueries value:
                                    HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprocserver32[]
                                    HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win64[]
  Queries value:
                                    HKCR\clsid\{c8e6f269-b90a-4053-a3be-
  Oueries value:
499afcec98c4}\inprocserver32[threadingmodel]
HKLM\software\microsoft\windows\currentversion\policies\system[enablelua]
                                    HKLM\software\microsoft\rpc[udtalignmentpolicy]
  Queries value:
  Queries value:
                                    HKCR\interface\{00020400-0000-0000-c000-00000000046}\proxystubclsid32[]
                                    HKCU\software\microsoft\windows\currentversion\action
  Oueries value:
center\checks\{c8e6f269-b90a-4053-a3be-499afcec98c4}.check.0[checksetting]
                                    HKCR\clsid\{00020420-0000-0000-c000-00000000046}[]
                                    HKCR\clsid\{00020420-0000-0000-c000-
  Oueries value:
00000000046}\inprocserver32[inprocserver32]
  Queries value:
                                    \label{local-equation} \mbox{HKCR\clsid\{00020420-0000-0000-c000-000000000046\}\inprocserver32[]}}
                                    HKCR\clsid\{00020420-0000-0000-c000-
  Oueries value:
00000000046}\inprocserver32[threadingmodel]
                                    HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}[]
  Queries value:
  Oueries value:
                                    HKCR \inf \{e3bf6178-694e-459f-a5a6-191ea0ffa1c7\} \inf \{e3bf6178-694e-459f-a5a6-191ea0ffa1c7\} 
  Oueries value:
                                    HKCR\clsid\{900c0763-5cad-4a34-bc1f-
40cd513679d5}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprocserver32[]
  Oueries value:
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\action
```

explorer\security[disablefixsecuritysettings]

```
center\providers\eventlog\{01979c6a-42fa-414c-b8aa-eee2c8202018}[lastknownstate]
                              HKCR\clsid\{900c0763-5cad-4a34-bc1f-
  Oueries value:
40cd513679d5}\inprocserver32[threadingmodel]
                               HKCR\interface\{e3bf6178-694e-459f-a5a6-191ea0ffa1c7}\typelib[]
  Queries value:
                               HKCR\interface\{e3bf6178-694e-459f-a5a6-191ea0ffa1c7}\typelib[version]
  Oueries value:
  Queries value:
                               HKCR \ | \ b722bccb-4e68-101b-a2bc-00aa00404770 \ | \ b722bccb-4e68-101b-a2bc-00aa0040470 \ | \ b722bccb-4e68-101b-a2bc-00aa004040 \ | \ b722bccb-4e68-101b-a2bc-00aa004040 \ | \ b722bccb-4e68-101b-a2bc-00aa004040 \ | \ b722bccb-4e68-101b-a2bc-00aa004040 \ | \ b722bccb-4e68-101b-a2bc-00aa0040 \ | \ b722bccb-4e68-101b-a2bc-00aa0040 \ 
  Oueries value:
                               HKCU \ software \ microsoft \ windows \ current version \ action
center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.100[checksetting]
                              HKCU\software\microsoft\windows\currentversion\action
  Queries value:
center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.101[checksetting]
                              HKCU\software\microsoft\windows\currentversion\action
  Oueries value:
center\providers\eventlog\{945a8954-c147-4acd-923f-40c45405a658}[lastknownstate]
  Oueries value:
                              HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}[]
                              HKCR\clsid\{a4a1a128-768f-41e0-bf75-
  Oueries value:
e4fddd701cba}\inprocserver32[inprocserver32]
  Queries value:
                              HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[]
                              HKCR\clsid\{a4a1a128-768f-41e0-bf75-
  Oueries value:
e4fddd701cba}\inprocserver32[threadingmodel]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\action
center\checks\{945a8954-c147-4acd-923f-40c45405a658}.check.42[checksetting]
                              HKCU\software\microsoft\windows\currentversion\action
  Queries value:
center\providers\eventlog\{dab69a6a-4d2a-4d44-94bf-e0091898c881}[lastknownstate]
  Oueries value:
                              HKCU\software\microsoft\windows\currentversion\action
center\checks\{dab69a6a-4d2a-4d44-94bf-e0091898c881}.check.100[checksetting]
                              HKCU\software\microsoft\windows\currentversion\action
  Queries value:
center\providers\eventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}[lastknownstate]
  Sets/Creates value:
                               HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-
409d6c4515e9}\inprocserver32[threadingmodel]
                              HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-
 Sets/Creates value:
409d6c4515e9}\inprocserver32[]
                              HKCU\software\microsoft\windows\currentversion\action
 Sets/Creates value:
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.106[checksetting]
                              HKLM\software\wow6432node\microsoft\direct3d\mostrecentapplication[name]
  Value changes:
  Value changes:
                               HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32[]
 Value changes:
Value changes:
Value changes:
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 \ 000000000007 \ [packed catalog item]
 Value changes:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries \ 0000000000006 \ [packed catalog item]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
 Value changes:
Value changes:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries \ 0000000000003 \ [packed catalog item]
  Value changes:
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
 Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010[packedcatalogitem]
  Value changes:
Value changes:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries 64 \ 000 000 000 000 8 \ [packed catalog item]
 Value changes:
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006[packedcatalogitem]
 Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005[packedcatalogitem]
 Value changes:
Value changes:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ catalog\_entries \ 4 \ 0000000000003 \ [packed catalog item]
 Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002[packedcatalogitem]
 Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001[packedcatalogitem]
 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\winsock2\parameters\namespace_catalog5\catalog_entries64\00000000005[librarypath]
 Value changes:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ (catalog\_entries 64 \ 000000000001[library path])
                               HKLM\system\currentcontrolset\services\browser[start]
Value changes:
```

Value changes: HKLM\system\currentcontrolset\services\policyagent[start]

Value changes: HKLM\software\microsoft\windows media player

nss\3.0\devices[alivedevicecount]

Value changes: HKLM\software\microsoft\windows media player

nss\3.0\devices[functionaldmrcount]

Value changes: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform[servicesessionid]

Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2\}.check.100[checksetting] Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2\}.check.101[checksetting] Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018\}.check.100[checksetting]