Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3331, Task ID: 833

Task ID: 833 Risk Level: 10

Date Processed: 2016-05-18 10:44:09 (UTC)

Processing Time: 62.45 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe"

Sample ID: Type: basic admin Owner:

1be5bc13fd1cf615a95feec0c5b7fd13 Label: 2016-05-18 10:30:52 (UTC)

Date Added: PE32:win32:gui

File Type: File Size: 201728 bytes

1be5bc13fd1cf615a95feec0c5b7fd13 MD5:

10e3f54492e5cdcdf2c1ae6d097aafdea9474ff77bf6ccb5a9c762ccb6e4a347 SHA256:

Description: None

Pattern Matching Results

Writes to memory of system processes

- Modifies registry autorun entries
- 6 Writes to system32 folder
- 5 Abnormal sleep detected
- Injects thread into Windows process
- 3 Connects to local host
- 6 Changes Winsock providers
- 10 Creates malicious events: ZeroAccess [Rootkit]
- 4 Terminates process under Windows subfolder
- 4 Reads process memory
- 3 Long sleep detected
- 5 Installs service

Process/Thread Events

Creates process: C:\windows\temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe

["C:\windows\temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe"]

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

Files\Windows Media Player\wmpnetwk.exe"]

PID:2644 C:\Windows\System32\calc.exe Reads from process: PID:1184 C:\Windows\explorer.exe Writes to process: Writes to process: PID:456 C:\Windows\System32\services.exe PID:2600 C:\Windows\System32\cmd.exe Writes to process:

C:\Windows\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe Terminates process:

Terminates process: C:\Windows\System32\cmd.exe C:\Windows\System32\rundll32.exe Terminates process:

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

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

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex \BaseNamedObjects\DBWinMutex Creates mutex:

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

\BaseNamedObjects\SvcctrlStartEvent A3752DX Creates event:

Creates event:

\BaseNamedObjects\ConsoleEvent-0x00000A38 Creates event: \BaseNamedObjects\TermSrvReadyEvent Creates event:

\BaseNamedObjects\{9360DA4B-0822-41F5-A360-7F9B7A2E9449} Creates event:

\KernelObjects\MaximumCommitCondition

File System Events

Creates C:\\$Recycle.Bin\

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

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

1002\\$b136cea6dd8900e373425c26f869789d

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

1002\\$b136cea6dd8900e373425c26f869789d\L

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

1002\\$b136cea6dd8900e373425c26f869789d\U

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

1002\\$b136cea6dd8900e373425c26f869789d\@

```
C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-
 Creates:
1002\$b136cea6dd8900e373425c26f869789d\n
 Creates:
                         C:\$Recycle.Bin\S-1-5-18
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d
 Creates:
 Creates:
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\L
 Creates:
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\U
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\@
 Creates:
 Creates:
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\n
 Creates:
                         C:GAC MSIL
 Creates:
                         C:\Windows\assembly\GAC\Desktop.ini
 Creates:
 Creates:
                         C: \verb|\windows\System32\LogFiles\Scm\5c2c622f-70e9-4194-a7da-033e827365ad|
 Creates:
                         C:\Windows\system32\catroot
 Creates:
                         C:\Windows\system32\catroot2
 Creates:
                         C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft
 Creates:
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player NSS\3.0
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player
NSS\3.0\SCPD
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player
NSS\3.0\Icon Files
 Opens:
                         C:\Windows\Prefetch\1BE5BC13FD1CF615A95FEEC0C5B7F-CFDFB467.pf
 Opens:
                         C:\Windows\System32
                         C:\Windows\System32\sechost.dll
 Opens:
 Opens:
                         C:\Windows\System32\imm32.dll
 Opens:
                         C:includeincludeincludeincludeinclude\
 Opens:
                         C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens:
                         C:\windows\temp\Cabinet.dll
 Opens:
                         C:\Windows\System32\cabinet.dll
 Opens:
                         C:\Windows\System32\mswsock.dll
 Opens:
                         C:\Windows\System32\WSHTCPIP.DLL
 Opens:
                         C:\windows\temp\CRYPTSP.dll
 Opens:
                         C:\Windows\System32\cryptsp.dll
 Opens:
                         C:\Windows\System32\rsaenh.dll
 Opens:
                         C:\windows\temp\CRYPTBASE.dll
 Opens:
                         C:\Windows\System32\cryptbase.dll
 Opens:
                         C:\Windows
 Opens:
                         C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-
1002\$b136cea6dd8900e373425c26f869789d\n
                         C:\Windows\MSWSOCK.dll
 Opens:
 Opens:
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\n
 Opens:
                         C:\Windows\assembly
 Opens:
                         C:\Windows\assembly\GAC\Desktop.ini
 Opens:
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\@
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\U
 Opens:
 Opens:
                         C:\Windows\System32\cmd.exe
 Opens:
                         C:\Windows\System32\apphelp.dll
                         C:\Windows\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe
 Opens:
 Opens:
                         C:\Windows\Prefetch\CMD.EXE-4A81B364.pf
 Opens:
                         C:
                         C:\Program Files
 Opens:
 Opens:
                         C:\Program Files\Adobe
 Opens:
                         C:\Program Files\Adobe\Reader 9.0
 Opens:
                         C:\Program Files\Adobe\Reader 9.0\Reader
 Opens:
                         C:\Windows\Branding
 Opens:
                         C:\Windows\Branding\Basebrd
                         C:\Windows\Branding\Basebrd\en-US
 Opens:
 Opens:
                         C:\Windows\Globalization
 Opens:
                         C:\Windows\Globalization\Sorting
 Opens:
                         C:\Windows\System32\en-US
 Opens:
                         C:\Windows\System32\ntdll.dll
 Opens:
                         C:\Windows\System32\kernel32.dll
 Opens:
                         C:\Windows\System32\apisetschema.dll
 Opens:
                         C:\Windows\System32\KernelBase.dll
 Opens:
                         C:\Windows\System32\locale.nls
 Opens:
                         C:\Windows\System32\msvcrt.dll
 Opens:
                         C:\Windows\System32\winbrand.dll
 Opens:
                         C:\Windows\System32\user32.dll
                         C:\Windows\System32\gdi32.dll
 Opens:
 Opens:
                         C:\Windows\System32\lpk.dll
 Opens:
                         C:\Windows\System32\usp10.dll
 Opens:
                         C:\Windows\System32\msctf.dll
 Opens:
                         C:\Windows\System32\en-US\cmd.exe.mui
 Opens:
                         C:\Windows\Branding\Basebrd\basebrd.dll
 Opens:
                         C:\Windows\Branding\Basebrd\en-US\basebrd.dll.mui
 Opens:
                         C:\Program Files\Adobe\Reader 9.0\Reader\icucnv36.dll
 Opens:
                         C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-
1002\$b136cea6dd8900e373425c26f869789d\@
 Opens:
                         C:\Windows\Temp
                         C:\Windows\System32\rundll32.exe
 Opens:
 Opens:
                         C:\Windows\AppPatch\sysmain.sdb
```

```
Opens:
                         C:\Windows\AppPatch\AcLayers.dll
 Opens:
                         C:\Windows\System32\sspicli.dll
 Opens:
                         C:\Windows\System32\userenv.dll
 Opens:
                         C:\Windows\System32\profapi.dll
 Opens:
                         C:\Windows\System32\winspool.drv
 Opens:
                         C:\Windows\System32\mpr.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\LogFiles\Scm\5c2c622f-70e9-4194-a7da-033e827365ad
 Opens:
                         C:\Windows\System32\calc.exe
 Opens:
                         C:\
 Opens:
                         C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp
                         C:\Windows\ServiceProfiles
 Opens:
 Opens:
                         C:\Windows\System32\sppsvc.exe
 Opens:
                         C:\Windows\Prefetch\SPPSVC.EXE-B0F8131B.pf
 Opens:
                         C:\Windows\System32\drivers
 Opens:
                         C:\Windows\System32\winevt
 Opens:
                         C:\Windows\System32\winevt\Logs
 Opens:
                         C:\Windows\System32\sppwinob.dll
 Opens:
                         C:\Windows\System32\advapi32.dll
 Opens:
                         C:\Windows\System32\rpcrt4.dll
 Opens:
                         C:\Windows\System32\ole32.dll
 Opens:
                         C:\Windows\System32\en-US\sppsvc.exe.mui
 Opens:
                         C:\Windows\System32\rpcss.dll
 Opens:
                         C:\Windows\System32\drivers\spsys.sys
 Opens:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-Bits-
Client%40perational.evtx
                         C:\Windows\System32\RpcRtRemote.dll
 Opens:
 Opens:
                         C:\Program Files\Windows Media Player\wmpnetwk.exe
 Opens:
                         C:\Windows\Prefetch\WMPNETWK.EXE-D9F2A96F.pf
 Opens:
                         C:\$Extend
 Opens:
                         C:\Program Files\Internet Explorer
 Opens:
                         C:\Program Files\Windows Media Player
 Opens:
                         C:\Program Files\Windows Media Player\en-US
 Opens:
                         C:\ProgramData
 Opens:
                         C:\ProgramData\Microsoft
                         C:\ProgramData\Microsoft\Network
 Opens:
 Opens:
                         C:\ProgramData\Microsoft\Network\Downloader
 Opens:
                         C:\ProgramData\Microsoft\Windows
 Opens:
                         C:\ProgramData\Microsoft\Windows\DRM
 Opens:
                         C:\Users
 Opens:
                         C:\Users\Admin
                         C:\Users\Admin\AppData
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Media Player
 Opens:
                         C:\Users\Admin\AppData\Local\Temp
 Opens:
                         C:\Windows\Fonts
                         C:\Windows\Performance
 Opens:
 Opens:
                         C:\Windows\Prefetch
 Opens:
                         C:\Windows\Prefetch\ReadyBoot
 Opens:
                         C:\Windows\ServiceProfiles\NetworkService
 Opens:
                         C:\Windows\ServiceProfiles\NetworkService\AppData
 Opens:
                         C:\Windows\ServiceProfiles\NetworkService\AppData\Local
 Opens:
                         C:\Windows\System32\catroot
 Opens:
                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
 Opens:
                         C:\Windows\System32\SMI
 Opens:
                         C:\Windows\System32\SMI\Store
 Opens:
                         C:\Windows\System32\SMI\Store\Machine
 Opens:
                         C:\Windows\System32\wbem
 Opens:
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80
 Opens:
                         C:\USERS\ADMIN\APPDATA\LOCAL\TEMP\ARMUI.INI
                         C:\Windows\System32\provsvc.dll
 Opens:
 Opens:
                         C:\Windows\System32\wmpmde.dll
 Opens:
                         C:\Windows\System32\MSMPEG2ENC.DLL
 Opens:
                         C:\Windows\System32\devenum.dll
 Opens:
                         C:\Windows\System32\msdmo.dll
 Opens:
                         C:\Windows\System32\oleaut32.dll
                         C:\Windows\System32\ws2_32.dll
 Opens:
 Opens:
                         C:\Windows\System32\nsi.dll
 Opens:
                         C:\Windows\System32\IPHLPAPI.DLL
 Opens:
                         C:\Windows\System32\winnsi.dll
 Opens:
                         C:\Windows\System32\shlwapi.dll
                         C:\Windows\System32\wtsapi32.dll
 Opens:
 Opens:
                         C:\Program Files\Windows Media Player\en-US\wmpnetwk.exe.mui
```

C:\Windows\Prefetch\RUNDLL32.EXE-39102DB5.pf

Opens:

```
C:\Windows\System32\winsta.dll
  Opens:
  Opens:
                                        C:\Windows\System32\ntmarta.dll
                                        C:\Windows\System32\Wldap32.dll
  Opens:
  Opens:
                                        C:\Windows\System32\wmdrmdev.dll
  Opens:
                                        C:\Windows\System32\drmv2clt.dll
  Opens:
                                        C:\Windows\System32\version.dll
  Opens:
                                        C:\Windows\System32\mfplat.dll
  Opens:
                                        C:\Windows\System32\avrt.dll
  Opens:
                                        C:\Windows\System32\setupapi.dll
  Opens:
                                        C:\Windows\System32\cfgmgr32.dll
  Opens:
                                        C:\Windows\System32\devobj.dll
  Opens:
                                        C:\Windows\System32\shell32.dll
  Opens:
                                        C:\Windows\System32\wintrust.dll
  Opens:
                                        C:\Windows\System32\crypt32.dll
  Opens:
                                        C:\Windows\System32\msasn1.dll
                                        C:\Windows\System32\en-US\setupapi.dll.mui
  Opens:
  Opens:
                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
  Opens:
                                        C:\ProgramData\Microsoft\Windows\DRM\drmstore.hds
  Opens:
                                        C:\Windows\System32\blackbox.dll
                                        C:\ProgramData\Microsoft\Windows\DRM\blackbox.bin
  Opens:
                                        C:\ProgramData\Microsoft\Windows\DRM\v3ks.sec
  Opens:
  Opens:
                                        C:\ProgramData\Microsoft\Windows\DRM\v3ks.bla
  Opens:
                                        C:\Windows\System32\clbcatq.dll
  Opens:
                                        C:\Windows\System32\upnp.dll
  Opens:
                                        C:\Windows\System32\winhttp.dll
  Opens:
                                        C:\Windows\System32\webio.dll
  Opens:
                                        C:\Windows\System32\ssdpapi.dll
                                        C:\Windows\System32\sxs.dll
  Opens:
  Opens:
                                        C:\Windows\System32\stdole2.tlb
  Opens:
                                        C:\Windows\System32\dhcpcsvc6.dll
  Opens:
                                        C:\Windows\System32\dhcpcsvc.dll
  Opens:
                                        C:\Windows\System32\wmp.dll
  Opens:
C: \verb|\windows| winsxs| x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80 \\ |\windows| windows_172d18a4386696c80 \\ |\windows| windows_172d18a438669660 \\ |\windows| windows_172d18a43866960 \\ |\windows| windows_172d18a4386690 \\ |\windows| wi
  Opens:
                                        C:\Windows\System32\dwmapi.dll
  Opens:
                                        C:\Windows\System32\wmploc.DLL
  Opens:
                                        C:\Windows\System32\en-US\wmploc.DLL.mui
  Opens:
                                        C:\Program Files\Internet Explorer\ieproxy.dll
  Opens:
                                        C:\Windows\System32\WindowsCodecs.dll
                                        C:\Users\Admin\AppData\Local\Microsoft\Media
  Opens:
Player\CurrentDatabase_372.wmdb
  Opens:
                                       C:\Windows\System32\netapi32.dll
  Opens:
                                        C:\Windows\System32\netutils.dll
  Opens:
                                        C:\Windows\System32\srvcli.dll
  Opens:
                                        C:\Windows\System32\wkscli.dll
  Opens:
                                        C:\Windows\System32\wmpps.dll
  Opens:
                                        C:\Windows\System32\httpapi.dll
  Opens:
                                        C:\Windows\System32\pcwum.dll
                                        C:\Windows\System32\wship6.dll
  Opens:
  Opens:
                                        C:\Windows\System32\WinSATAPI.dll
  Opens:
                                        C:\Windows\System32\dxgi.dll
                                        C:\Windows\System32\en-US\WinSATAPI.dll.mui
  Opens:
  Opens:
                                        C:\Windows\System32\winmm.dll
  Opens:
                                        C:\Windows\System32\netprofm.dll
  Opens:
                                        C:\Windows\System32\nlaapi.dll
  Opens:
                                        C:\Windows\System32\npmproxy.dll
  Opens:
                                        C:\Windows\System32\upnphost.dll
  Opens:
                                        C:\Windows\System32\wbem\wbemprox.dll
  Opens:
                                        C:\Windows\System32\wbemcomn.dll
  Opens:
                                        C:\Windows\System32\wbem\wbemsvc.dll
  Opens:
                                        C:\Windows\System32\wbem\fastprox.dll
  Opens:
                                        C:\Windows\System32\ntdsapi.dll
  Opens:
                                        C:\Windows\System32\gpapi.dll
  Opens:
                                        C:\Windows\System32\FirewallAPI.dll
  Opens:
                                        C:\Windows\System32\en-US\KernelBase.dll.mui
  Opens:
                                        C:\Windows\System32\credssp.dll
  Opens:
                                        C:\Windows\System32\msxm13.d11
  Opens:
                                        C:\Windows\System32\msxml3r.dll
  Opens:
                                        C:\Windows\System32\dnsapi.dll
                                        {\tt C:\Windows\System32\urlmon.dll}
  Opens:
  Opens:
                                        C:\Windows\System32\wininet.dll
  Opens:
                                        C:\Windows\System32\iertutil.dll
  Opens:
                                        C:\Windows\Fonts\simfang.ttf
  Opens:
                                        C:\Windows\System32\wsock32.dll
  Opens:
                                        C:\ProgramData\Microsoft\Network\Downloader\qmgr1.dat
                                        C:\Windows\System32\powrprof.dll
  Opens:
  Opens:
                                        C:\Windows\System32\drivers\raspppoe.sys
  Opens:
                                        C:\Windows\System32\drivers\ndistapi.sys
  Opens:
                                        C:\Windows\System32\perfmon.exe
  Opens:
                                        C:\Windows\System32\cleanmgr.exe
                                        C:\Windows\System32\charmap.exe
  Opens:
  Opens:
                                        C:\WINDOWS\PREFETCH\READYBOOT\TRACE1.FX
```

```
816d-001c23e25b76}.TM.blf
                         C:\Windows\System32\SMI\Store\Machine\SCHEMA.DAT
 Opens:
                         C:\Windows\System32\en-US\FirewallAPI.dll.mui
 Opens:
 Opens:
                         C:\Program Files\Windows Media Player\WSOCK32.dll
 Opens:
                         C:\Program Files\Windows Media Player\IPHLPAPI.DLL
                         C:\Program Files\Windows Media Player\WINNSI.DLL
 Opens:
                         C:\Program Files\Windows Media Player\USERENV.dll
 Opens:
 Opens:
                         C:\Program Files\Windows Media Player\profapi.dll
                         C:\Program Files\Windows Media Player\WTSAPI32.dll
 Opens:
 Opens:
                         C:\Program Files\Windows Media Player\CRYPTBASE.dll
 Opens:
                         C:\Program Files\Windows Media Player\POWRPROF.DLL
 Opens:
                         C:\Program Files\Windows Media Player\WINSTA.dll
                         C:\Program Files\Windows Media Player\ntmarta.dll
 Opens:
 Opens:
                         C:\Program Files\Windows Media Player\wmdrmdev.dll
 Opens:
                         C:\Program Files\Windows Media Player\drmv2clt.dll
 Opens:
                         C:\Program Files\Windows Media Player\VERSION.dll
 Opens:
                         C:\Program Files\Windows Media Player\MFPlat.DLL
 Opens:
                         C:\Program Files\Windows Media Player\AVRT.dll
 Opens:
                         C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
 Opens:
                         C:\Windows\System32\catroot2
 Opens:
{\tt C:\Windows\Service\Profiles\Network\Service\AppData\Local\Microsoft\Windows\ Media\ Player\ NSS\3.0}
 Opens:
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player NSS
 Opens:
{\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\Icon Files\0aef9a97-98cd-4f89-b183-3db737149306.png
{\tt C:\Windows\Service\Profiles\Network\Service\AppData\Local\Microsoft\Windows\ Media\ Player}
NSS\3.0\SCPD
 Opens:
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player
NSS\3.0\0AEF9A97-98CD-4F89-B183-3DB737149306.xml
 Opens:
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player
NSS\3.0\Icon Files\0AEF9A97-98CD-4F89-B183-3DB737149306.ico
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player
NSS\3.0\Icon Files\0AEF9A97-98CD-4F89-B183-3DB737149306.jpg
 Opens:
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player
NSS\3.0\Icon Files\0AEF9A97-98CD-4F89-B183-3DB737149306.tif
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player
NSS\3.0\Icon Files\0AEF9A97-98CD-4F89-B183-3DB737149306.bmp
 Opens:
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player
NSS\3.0\Icon Files\0AEF9A97-98CD-4F89-B183-3DB737149306.gif
                         C:\Program Files\Windows Media Player\CRYPTSP.dll
 Opens:
                         C:\Program Files\Windows Media Player\RpcRtRemote.dll
 Opens:
 Opens:
                         C:\Program Files\Windows Media Player\SXS.DLL
 Opens:
                         C:\Windows\System32\spp\plugin-manifests-signed\sppwinob-spp-plugin-
manifest-signed.xrm-ms
 Writes to:
                         C:\$Recvcle.Bin\S-1-5-21-2160590473-689474908-1361669368-
1002\$b136cea6dd8900e373425c26f869789d\@
                         C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-
1002\$b136cea6dd8900e373425c26f869789d\n
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\@
 Writes to:
 Writes to:
                         C:\Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\n
 Writes to:
                         C:\Windows\assembly\GAC\Desktop.ini
                         C:\Windows\System32\LogFiles\Scm\5c2c622f-70e9-4194-a7da-033e827365ad
Writes to:
 Reads from:
                         C:\Windows\Prefetch\CMD.EXE-4A81B364.pf
 Reads from:
                         C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\@
                         C: \verb|\windows\System32\LogFiles\Scm\5c2c622f-70e9-4194-a7da-033e827365ad|
 Reads from:
 Reads from:
                         C:\Windows\Prefetch\SPPSVC.EXE-B0F8131B.pf
 Reads from:
                         C:\Windows\Prefetch\WMPNETWK.EXE-D9F2A96F.pf
 Reads from:
                         C:\ProgramData\Microsoft\Windows\DRM\drmstore.hds
                         C:\ProgramData\Microsoft\Windows\DRM\blackbox.bin
 Reads from:
 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
 Reads from:
                         C:\Windows\Svstem32\stdole2.tlb
 Reads from:
                         C:\Windows\System32\spp\plugin-manifests-signed\sppwinob-spp-plugin-
manifest-signed.xrm-ms
 Deletes:
                         C:\Windows\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe
 Deletes:
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player
```

NSS\3.0\Icon Files\0aef9a97-98cd-4f89-b183-3db737149306.png

C:\Windows\System32\SMI\Store\Machine\SCHEMA.DAT{e29ac73d-7037-11de-

Opens:

Network Events

DNS query: DNS response:	<pre>j.maxmind.com j.maxmind.com ⇒ 127.0.0.1</pre>
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:	68.185.188.253:16471
Sends data to:	189.68.16.1:16471
Sends data to:	
	109.53.87.1:16471
Sends data to:	68.49.152.252:16471
Sends data to: Sends data to:	80.109.74.3:16471
Sends data to:	130.204.226.4:16471
Sends data to:	221.244.148.250:16471 176.227.128.250:16471
Sends data to:	
Sends data to:	173.80.73.5:16471
Sends data to:	74.210.157.7:16471
Sends data to:	180.47.189.7:16471 74.56.221.248:16471
Sends data to:	
	37.192.19.8:16471
Sends data to: Sends data to:	68.119.104.8:16471 98.200.249.8:16471
Sends data to:	37.4.80.10:16471
Sends data to:	187.14.203.11:16471
Sends data to:	68.16.8.248:16471
Sends data to:	176.200.253.13:16471
Sends data to:	72.177.97.245:16471
Sends data to:	77.0.111.14:16471
Sends data to:	174.5.197.15:16471
Sends data to:	76.24.211.244:16471
Sends data to:	70.119.200.15:16471
Sends data to:	108.129.22.18:16471
Sends data to:	96.30.133.20:16471
Sends data to:	67.163.238.20:16471
Sends data to:	72.204.20.22:16471
Sends data to:	190.219.25.242:16471
Sends data to:	98.121.198.241:16471
Sends data to:	200.127.18.241:16471
Sends data to:	79.114.143.240:16471
Sends data to:	217.209.199.22:16471
Sends data to:	180.31.88.23:16471
Sends data to:	77.103.179.238:16471
Sends data to:	146.247.84.238:16471
Sends data to:	124.123.122.236:16471
Sends data to:	69.204.104.236:16471
Sends data to:	98.196.20.25:16471
Sends data to:	109.192.63.25:16471
Sends data to:	151.43.129.233:16471
Sends data to:	97.106.93.233:16471
Sends data to:	61.192.120.25:16471
Sends data to:	68.35.204.26:16471
Sends data to:	75.74.160.229:16471
Sends data to:	190.178.170.27:16471
Sends data to:	95.223.50.224:16471
Sends data to:	174.134.97.223:16471
Sends data to:	79.114.25.28:16471
Sends data to:	88.129.134.29:16471
Sends data to:	86.124.233.220:16471
Sends data to:	5.35.105.220:16471
Receives data from:	0.0.0.0:0

Windows Registry Events

Creates key:	HKCU\software\classes\clsid
Creates key:	HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}
Creates key:	HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-
409d6c4515e9}\inpr	ocserver32
Creates key:	HKLM\system\currentcontrolset\services\eventlog\system\wmpnetworksvc
Creates key:	HKLM\system
Creates key:	HKLM\system\currentcontrolset
Creates key:	HKLM\system\currentcontrolset\services
Creates key:	HKLM\system\currentcontrolset\services\eventlog
Creates key:	HKLM\system\currentcontrolset\services\eventlog\system
Creates key:	<pre>HKLM\software\microsoft\windows media player nss\3.0\events</pre>
Creates key:	<pre>HKLM\software\microsoft\windows media player nss\3.0\events\{9360da4b-</pre>
0822-41f5-a360-7f9	b7a2e9449}
Creates key:	<pre>HKLM\software\microsoft\cryptography\rng</pre>
Creates key:	<pre>HKLM\software\microsoft\windows media player nss\3.0\servers</pre>
Creates key:	HKLM\software\microsoft\windows media player nss\3.0\events\{6cc10660-
1516-4ed8-94f7-9ca	dbee645b1}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}
Creates key:	<pre>HKLM\software\microsoft\windows media player nss\3.0\events\{9360da4b-</pre>
0822_41f5_a360_7f0	h732e0110\\ \h6f6810f_0ce1_1380_he1h_e9c93f9f133h\

 $0822-41f5-a360-7f9b7a2e9449\} \setminus \{b6f6840f-0ce4-4389-be1b-e9c93f9f433b\}$

Creates key: 00-00-00

Creates key: HKLM\software\microsoft\windows media player nss\3.0\devices\08-00-27-

ca-8f-e0

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

Deletes value: HKLM\software\microsoft\windows media player nss\3.0\servers[0aef9a97-

98cd-4f89-b183-3db737149306]

Deletes value: HKLM\software\microsoft\windows media player nss\3.0\server settings\s-

1-5-21-2160590473-689474908-1361669368-1002[0aef9a97-98cd-4f89-b183-3db737149306]

Opens key: HKLM\system\currentcontrolset\control\session manager

Opens key: HKLM\system\currentcontrolset\control\terminal server

Opens key: HKLM\system\currentcontrolset\control\safeboot\option

Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll

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

Opens key: HKCU\

Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration

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

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key: HKLM\system\currentcontrolset\control\error message instrument\
Opens key: HKLM\system\currentcontrolset\control\error message instrument
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility

Opens key: HKLM\

Opens key: HKLM\software\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\software\policies\microsoft\sqmclient\windows

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

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

 $Opens\ key: \\ HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ appid_catalog$

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\1e6c4482
Opens key:

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019
Opens key:

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

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

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

 $\label{lem:hklmsystem} HkLM \system \current controls et \services \winsock 2 \parameters \protocol_catalog 9 \catalog_entries \000000000011 \parameters \end{substitute} Opens key:$

 $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \protocol_catalog 9 \catalog_entries \000000000012 \parameters \end{subarray} Opens \ key:$

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014
Opens key:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \protocol_catalog 9 \catalog_entries \0000000000015 \parameters \end{substitute} Opens key:$

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018
Opens kev:

Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries Opens kev: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006 Opens key: HKLM\svstem\currentcontrolset\services\winsock\parameters Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock Opens key: HKLM\system\currentcontrolset\services\psched\parameters\winsock Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\psched HKLM\system\currentcontrolset\services\tcpip\parameters\winsock Opens kev: Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip HKLM\software\microsoft\cryptography\defaults\provider\microsoft base Opens key: cryptographic provider v1.0 Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy Opens key: HKLM\system\currentcontrolset\control\lsa Opens key: HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration HKLM\software\policies\microsoft\cryptography Opens key: Opens key: HKLM\software\microsoft\cryptography Opens key: HKLM\software\microsoft\cryptography\offload Opens key: ${\tt HKLM \setminus software \setminus microsoft \setminus cryptography \setminus deshash session keybackward}$ Opens key: HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprocserver32 HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprocserver32 Opens key: Opens key: $HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ objects \ \{7007acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3202-11d1-1207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207acc7-3207ac$ aad2-00805fc1270e} Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{21ec2020-3aea-1069-a2dd-08002b30309d\}$ Opens key: HKCR\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d} Opens key: $HKLM \setminus software \setminus irrosoft \setminus ir$ a2dd-08002b30309d} Opens key: $HKCU \ software \ microsoft \ windows \ current version \ explorer \ desktop \ namespace \ \{21ec 2020 - 3aea - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1069 - 1$ a2dd-08002b30309d} HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e} Opens key: Opens key: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e} Opens key: $HKLM \ software \ microsoft \ windows \ current version \ explorer \ control panel \ namespace \ \{7007acc7-3202-12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014, 12014,$ 11d1-aad2-00805fc1270e} Opens kev: 11d1-aad2-00805fc1270e} HKCU\software\classes\clsid\{2227a280-3aea-1069-a2de-08002b30309d} Opens key: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d} Opens key: Opens key: $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus explorer \setminus clsid \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus explorer \setminus clsid \setminus explorer \setminus clsid$ 3aea-1069-a2de-08002b30309d} Opens key: HKCU\system\currentcontrolset\control\network\showwirelessconnectingonstart HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1 Opens kev: Opens key: $HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in foll control panel \ name space \ name customizations$ Opens key: HKLM\system\currentcontrolset\control\mui\stringcachesettings $HKCU \setminus software \setminus classes \setminus local\ settings \setminus muicache \setminus 27 \setminus 52c64b7e$ Opens key: Opens key: $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \clsid \closer{local_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammo$ 3202-11d1-aad2-00805fc1270e} $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ Opens key: options\dllnxoptions Opens kev: 9a6f-135d9c6622cc} Opens kev: a949-c1b91af43b1a}

Opens key: HKLM\system\setup
Opens key: HKLM\software\policies\microsoft\windows nt\rpc

HKLM\software\microsoft\rpc

HKLM\software\microsoft\windows\currentversion\run

Opens key:

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

Opens key: HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\cmd.exe

Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility

Opens key: HKLM\software\policies\microsoft\windows\appcompat
Opens key: HKCU\software\microsoft\windows nt\currentversion

Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers

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

Opens key: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags\custom\cmd.exe

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

options

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist
Opens key: HKLM\system\currentcontrol\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

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

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

options\rundll32.exe

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

nt\currentversion\appcompatflags\layers

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

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: HKCU\software\microsoft\windows nt\currentversion\appcompatflags

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

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

 $\label{thm:linear} Opens~key: \\ HKLM\system\currentcontrolset\control\networkprovider\hworder$

Opens key: $\mbox{HKLM} \mbox{system} \mbox{currentcontrolset} \mbox{services} \mbox{bfe}$

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: ${\tt HKLM \backslash system \backslash current control set \backslash services \backslash appinfo \backslash triggerinfo}$

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\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: ${\tt HKLM \ } {\tt System \ } {\tt current controlset \ } {\tt bthserv}$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

HKLM\system\currentcontrolset\services\wcspluginservice\triggerinfo

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

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

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

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

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

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

535773d48449}\progid

535773d48449}\inprocserver32

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

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

535773d48449}\inprochandler32

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

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

535773d48449}\inprochandler

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

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

Opens key: HKCR\applications\calc.exe

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

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

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

0000f87a470c}\treatas

Opens key: $\begin{tabular}{ll} HKCR\clsid\dd313e04-feff-11d1-8ecd-0000f87a470c\treatas \\ Opens key: \\ HKCU\software\classes\clsid\dd313e04-feff-11d1-8ecd- \\ \end{tabular}$

0000f87a470c}\progid

Opens key: $\begin{tabular}{ll} HKCR\clsid\\{dd313e04-feff-11d1-8ecd-0000f87a470c}\\ Progid\\ HKCU\software\\classes\\clsid\\{dd313e04-feff-11d1-8ecd-0000f87a470c}\\ HKCU\software\\clsid\\{dd313e04-feff-11d1-8ecd-00000f87a470c}\\ HKCU\software\\clsid\\{dd313e04-feff-11d1-8ecd-0000f87a470c}\\ HKCU\software\\clsid\\{dd313e04-feff-11d1-8ecd-0000f87a470$

0000f87a470c}\inprocserver32

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

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

0000f87a470c}\inprochandler32

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

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

0000f87a470c}\inprochandler

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

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in folders$

Opens key: HKLM\software\microsoft\windows\currentversion\explorer\user shell

folders

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

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-20 Opens key: HKU\s-1-5-20\software\microsoft\windows\currentversion\explorer\user

shell folders

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

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

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

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

Opens key: HKCU\software\classes\
Opens key: HKLM\software\classes
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

 $\verb|nt\currentversion\software| protection platform \\$

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

options\wmpnetwk.exe

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

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

Opens key: HKCR\appid\wmpnetwk.exe

Opens key: HKLM\software\microsoft\windows\error reporting\wmr
Opens key: HKLM\software\microsoft\windows\currentversion\setup
Opens key: HKLM\software\policies\microsoft\windowsmediaplayer

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

Opens key: HKCR\clsid\{02e6ec4c-96e4-42e8-b533-336916a0087d}

Opens key: HKCR\clsid\{02e6ec4c-96e4-42e8-b533-336916a0087d}\inprochandler32
Opens key: HKCR\clsid\{02e6ec4c-96e4-42e8-b533-336916a0087d}\inprochandler
Opens key: HKLM\system\currentcontrol\sa\accessproviders

```
Opens key:
                                    HKLM\system\currentcontrolset\services\ldap
                                    HKLM\software\microsoft\windows media foundation\platform
  Opens key:
  Opens kev:
                                    HKLM\system\currentcontrolset\services\crypt32
                                    HKLM\software\microsoft\windows nt\currentversion\msasn1
  Opens key:
  Opens key:
                                    HKLM\software\microsoft\drm
  Opens key:
                                    HKLM\software\microsoft\cryptography\oid
                                    HKLM\software\microsoft\cryptography\oid\encodingtype 0
  Opens key:
                                    {\tt HKLM \ } software \verb|\ microsoft \ \\ cryptography \verb|\ oid \ \\ encoding type \\
  Opens key:
0\cryptdlldecodeobjectex
  Opens key:
                                    HKLM\software\microsoft\cryptography\oid\encodingtype 1
                                    HKLM\software\microsoft\cryptography\oid\encodingtype
  Opens kev:
1\cryptdlldecodeobjectex
  Opens key:
                                    HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.1.1
  Opens key:
                                    HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.1
                                    HKLM\software\microsoft\cryptography\oid\encodingtype
  Opens kev:
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
  Opens key:
                                    HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.2
                                    HKLM\software\microsoft\cryptography\oid\encodingtype
  Opens kev:
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:
                                    \label{lem:hklm} \mbox{ HKLM\software\mbox{\sc media player nss\sc ontrol}} \mbox{ 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\08-00-27-
ca-8f-e0
  Opens key:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions
9d55-7b8e7f157091}
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}\propertybag
  Opens key:
                                    HKCU\software\microsoft\windows\currentversion\explorer
                                    HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus session in fo \setminus 0
  Opens key:
  Opens key:
                                    HKCU\control panel\international
  Opens kev:
\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} windows \end{tabular} current version \end{tabular} explorer \end{tabular} known folders ettings
                                    HKLM\software\microsoft\windows media player nss\3.0\server settings
  Opens kev:
  Opens key:
                                    HKLM\software\microsoft\windows media player nss\3.0\servers\0aef9a97-
98cd-4f89-b183-3db737149306
  Opens key:
                                    HKLM\software\microsoft\windows media player nss\3.0\server settings\s-
1-5-21-2160590473-689474908-1361669368-1002
                                    HKLM\software\microsoft\windows\ media\ player\ nss\3.0\events\{6cc10660-microsoft\windows\ media\ player\ nss\3.0\events\}
  Opens key:
1516-4ed8-94f7-9cadbee645b1}
  Opens key:
                                    HKLM\software\microsoft\windows media player nss\3.0\events\{6cc10660-
1516-4ed8-94f7-9cadbee645b1}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}
                                    HKLM \setminus software \setminus microsoft \setminus windows \ media \ player \ nss \setminus 3.0 \setminus events \setminus \{9360 da4b-100 da4b-10
  Opens key:
0822-41f5-a360-7f9b7a2e9449}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}
  Opens key:
                                    HKLM\software\microsoft\com3
                                    HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}
  Opens key:
  Opens key:
                                    HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}\treatas
                                    HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}\progid
  Opens key:
  Opens key:
                                    HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}\inprocserver32
  Opens key:
                                    HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}\inprochandler32
  Opens key:
                                    HKCR \ clsid \ \{e2085f28-feb7-404a-b8e7-e659bdeaaa02\} \ \ inprochandler
  Opens key:
                                    HKCR\interface\{00000134-0000-0000-c000-00000000046}
  Opens key:
                                    HKCR\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32
                                    HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}
  Opens key:
  Opens key:
                                    HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}\proxystubclsid32
  Opens key:
                                    HKCR\clsid\{00020424-0000-0000-c000-00000000046}
                                    HKCR\clsid\{00020424-0000-0000-c000-00000000046}\treatas
  Opens key:
  Opens key:
                                    HKCR\clsid\{00020424-0000-0000-c000-00000000046}\progid
  Opens key:
                                    HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprocserver32
                                    Opens key:
  Opens key:
                                    HKCR\clsid\{00020424-0000-0000-c000-00000000046}\ inprochandler
  Opens key:
                                    HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}\forward
  Opens key:
                                    HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}\typelib
  Opens key:
                                    HKCR\typelib\{db3442a7-a2e9-4a59-9cb5-f5c1a5d901e5}
                                    HKCR\typelib\{db3442a7-a2e9-4a59-9cb5-f5c1a5d901e5}\1.0
  Opens kev:
  Opens key:
                                    HKCR\typelib\{db3442a7-a2e9-4a59-9cb5-f5c1a5d901e5}\1.0\0
  Opens key:
                                    HKCR\typelib\{db3442a7-a2e9-4a59-9cb5-f5c1a5d901e5}\1.0\0\win32
  Opens key:
                                    HKCR\typelib
                                    HKCR\typelib\{00020430-0000-0000-c000-00000000046}
  Opens key:
  Opens key:
                                    HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0
                                    HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0
  Opens kev:
  Opens key:
```

```
HKCR\interface\{00020400-0000-0000-c000-00000000046}\proxystubclsid32
        Opens key:
                                                                                                              HKCR\clsid\{00020420-0000-0000-c000-00000000046}
        Opens kev:
                                                                                                              HKCR\clsid\{00020420-0000-0000-c000-00000000046}\treatas
        Opens key:
        Opens key:
                                                                                                              HKCR\clsid\{00020420-0000-0000-c000-00000000046}\progid
        Opens key:
                                                                                                              Opens key:
                                                                                                              HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprochandler
        Opens key:
        Opens key:
                                                                                                              HKCR\interface\{e3bf6178-694e-459f-a5a6-191ea0ffa1c7}
                                                                                                              HKCR\ interface \ \{e3bf6178-694e-459f-a5a6-191ea0ffa1c7\}\ proxystubclsid 32
        Opens key:
                                                                                                             HKLM\software\microsoft\windows
        Opens kev:
nt\currentversion\softwareprotectionplatform\plugins\modules
        Opens key:
                                                                                                            HKLM\software\microsoft\windows
nt \verb|\current version| software protection platform \verb|\plugins| modules \verb|\normal| 19b8a65-b0f6-41d9-acea-12006ef9b32a | and the protection platform \verb|\plugins| modules \verb|\normal| 19b8a65-b0f6-41d9-acea-12006ef9b32a | and the protection platform \verb|\plugins| modules \verb|\normal| 19b8a65-b0f6-41d9-acea-12006ef9b32a | and the protection platform \verb|\plugins| modules \verb|\normal| 19b8a65-b0f6-41d9-acea-12006ef9b32a | and the protection platform \verb|\plugins| modules modu
        Opens key:
                                                                                                             HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\modules\c42d83ff-5958-4af4-a0dd-ba02fed39662
                                                                                                            HKCR\interface\{e3bf6178-694e-459f-a5a6-191ea0ffa1c7}\forward
        Opens kev:
        Opens key:
                                                                                                             HKCR\interface\{e3bf6178-694e-459f-a5a6-191ea0ffa1c7}\typelib
        Opens key:
                                                                                                             HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects
        Opens key:
                                                                                                             HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/bios/4.0
                                                                                                            HKLM\software\microsoft\windows
        Opens kev:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/flags/1.0
       Opens key:
                                                                                                             HKLM\software\microsoft\windows
nt \verb|\currentversion| software protection platform \verb|\plugins| objects \verb|\msft:rm/algorithm/hwid/4.0| | the protection platform objects \verb|\msft:rm/algorithm/hwid/4.0| | the protection objects o
                                                                                                             HKLM\software\microsoft\windows
        Opens key:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/phone/1.0
                                                                                                             HKLM\software\microsoft\windows
        Opens kev:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2005
                                                                                                             HKLM\software\microsoft\windows
       Opens kev:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/vmd/1.0
                                                                                                             HKLM\software\microsoft\windows
        Opens key:
nt \verb|\currentversion| software protection platform \verb|\plugins| objects \verb|\msft:rm/algorithm/volume/1.0| and the province of the property of 
        Opens key:
                                                                                                            HKLM\software\microsoft\windows
nt \verb|\currentversion| software protection platform \verb|\plugins| objects \verb|\msft|: spp/license acquisition/payload handler/eul/1.0 | and the protection of the property of the
       Opens kev:
                                                                                                             HKLM\software\microsoft\windows
nt \verb|\currentversion| software protection platform \verb|\plugins| objects \verb|\msft|: spp/license acquisition/payload handler/pkc/1.0
                                                                                                             HKLM\software\microsoft\windows
        Opens key:
nt \verb|\current| version \verb|\software| protection platform \verb|\plug| ins \verb|\software| plugins software| plugins s
        Opens key:
                                                                                                             HKLM\software\microsoft\windows
nt \verb|\currentversion| software protection platform \verb|\plugins| sobjects \verb|\msft|: spp/license acquisition/payload handler/spc/1.0 | and the protection of the property of th
       Opens kev:
                                                                                                             HKLM\software\microsoft\windows
nt \verb|\current| version \verb|\soft| ware protection platform \verb|\plugins| objects \verb|\msft|: spp/license acquisition/sequence/1.0 | the province of the property of the province o
                                                                                                             HKLM\software\microsoft\windows
        Opens kev:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/taskscheduler/1.0
        Opens key:
                                                                                                             HKLM\software\microsoft\windows
nt \verb|\currentversion| software protection platform \verb|\plugins| objects \verb|\msft:spp/volume/services/kms/1.0| is a superior of the provided by the property of the provided by the provided by
                                                                                                            HKLM\software\microsoft\windows
       Opens kev:
nt \verb|\currentversion| software protection platform \verb|\plugins| objects \verb|\msft:spp/volume/services/kms/licenserenewal/1.0| and the protection platform of the property of th
                                                                                                            HKLM\software\microsoft\windows
        Opens kev:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/windowsfunctionality/agent/7.0
        Opens key:
                                                                                                            HKCR\interface\{0405af4f-8b5c-447c-80f2-b75984a31f3c}
                                                                                                              HKCR \verb|\interface| \{0405af4f-8b5c-447c-80f2-b75984a31f3c\} \verb|\proxystubclsid32| \} |
        Opens key:
        Opens kev:
                                                                                                             HKCR\interface\{0405af4f-8b5c-447c-80f2-b75984a31f3c}\forward
        Opens key:
                                                                                                             HKCR\interface\{0405af4f-8b5c-447c-80f2-b75984a31f3c}\typelib
                                                                                                             Oueries value:
manager[cwdillegalindllsearch]
                                                                                                             HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
        Oueries value:
        Queries value:
                                                                                                             HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
        Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
                                                                                                             HKCU\control panel\desktop[preferreduilanguages]
        Queries value:
                                                                                                             HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
        Oueries value:
        Oueries value:
HKLM \verb|\software\microsoft\windows \verb|\currentversion\side| preferex ternal 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]
        Queries value:
                                                                                                            HKLM\software\microsoft\windows
nt\currentversion\compatibility32[1be5bc13fd1cf615a95feec0c5b7fd13]
                                                                                                           HKLM\software\microsoft\windows
       Oueries value:
nt\currentversion\windows[loadappinit_dlls]
        Queries value:
                                                                                                            HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
        Oueries value:
                                                                                                             HKLM\svstem\currentcontrolset\control\nls\extendedlocale[en-us]
        Queries value:
                                                                                                             HKLM\software\microsoft\sqmclient\windows[ceipenable]
        Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
        Oueries value:
```

HKCR\interface\{00020400-0000-0000-c000-00000000046}

Opens key:

Oueries value:

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

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
 Oueries value:

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

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000002[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem] Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ catalog_entries \ 000000000011 \ [packed catalog item] \ Queries \ value:$
- $HKLM \system \current control set \services \winsock 2 \parameters \protocol_catalog 9 \catalog_entries \noon 000000000012 \packed catalog item] \\ Queries value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[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\00000000001[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[addressfamily] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
 Oueries value:
- 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] Queries value:
- $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace_catalog \ set alog_entries \ 00000000000002 [provider info] \ Queries \ value:$
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 000000000003 [library path] \\ Queries \ value:$

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
 Oueries 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\000000000003[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[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\0000000000004[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000005[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\00000000005[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerinfo]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[librarypath] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[version]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries \ 000000000006 \ [storesserviceclass info] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
 Oueries value:
- $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws 2_32 numhandle buckets]$

Queries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
- Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip6 \setminus parameters \setminus winsock [mapping]$

- HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping]

 Queries value: HKLM\system\currentcontrolset\services\winsock\setup
- migration\providers\psched[winsock 2.0 provider id]
- Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
- Queries value: HKLM\system\currentcontrolset\services\winsock\setup
- migration\providers\tcpip[winsock 2.0 provider id]

Oueries value:

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

Oueries value:

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

Oueries value:

Oueries value:

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

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

cryptographic provider v1.0[type]

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

cryptographic provider v1.0[image path]

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

manager[safeprocesssearchmode]

Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled] Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy] Oueries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]

Queries value:

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

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

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

HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprocserver32[] Queries value:

HKCR\clsid\{7007acc7-3202-11d1-aad2-Oueries value:

00805fc1270e}\inprocserver32[loadwithoutcom]

HKCR\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}[sortorderindex] Queries value: $\label{local-equation} \mbox{HKCR\clsid} \mbox{\{7007acc7-3202-11d1-aad2-00805fc1270e\}[sortorderindex]}$ Queries value:

Queries value: HKCR\clsid\{2227a280-3aea-1069-a2de-

08002b30309d}[system.itemnamedisplay]

HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}[{b725f130-47ef-101a-Oueries value:

a5f1-02608c9eebac} 10]

Queries value: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}[localizedstring]

Queries value:

 $HKLM \setminus system \setminus current control \setminus mui \setminus string cache settings [string cache generation] \\$

Queries value: HKCU\software\classes\local

settings\muicache\27\52c64b7e[@c:\windows\system32\prnfldr.dll,-8036]

HKCR\clsid\{7007acc7-3202-11d1-aad2-Queries value:

00805fc1270e}[system.itemnamedisplay]

HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[{b725f130-47ef-101a-Oueries value:

a5f1-02608c9eebac} 10]

HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[localizedstring] Queries value:

Oueries value: HKCU\software\classes\local

settings\muicache\27\52c64b7e[@c:\windows\system32\netshell.dll,-1200]

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

options\dllnxoptions[usefilter]

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

options\dllnxoptions[n]

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

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

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

HKLM\system\setup[systemsetupinprogress]

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

Queries value:

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

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

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

 $\label{lem:hklm} \mbox{HKLM\software\mbox{\sc microsoft\windows}\ nt\current\sc version\sc mage file execution}$ Oueries value:

options[disablelocaloverride]

Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[cmd]

Oueries value: HKLM\system\currentcontrolset\control\cmf\config[system]

HKLM\software\microsoft\windows Queries value:

nt\currentversion\profilelist[programdata]

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

18[profileimagepath]

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

shell folders[appdata]

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

shell folders[local appdata]

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

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

nt\currentversion\compatibility32[rundll32]

Oueries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap] HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Oueries value: Queries value: HKLM\system\currentcontrolset\services\bfe[imagepath] Queries value: HKLM\system\currentcontrolset\services\bfe[type] Oueries value: HKLM\svstem\currentcontrolset\services\bfe[start] Queries value: HKLM\system\currentcontrolset\services\bfe[errorcontrol] Oueries value: HKLM\system\currentcontrolset\services\bfe[tag] Oueries value: HKLM\system\currentcontrolset\services\bfe[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\bfe[dependongroup] Oueries value: HKLM\system\currentcontrolset\services\bfe[group] Oueries value: HKLM\system\currentcontrolset\services\bfe[objectname] Queries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[action] Oueries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[type] Oueries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[guid] Oueries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[datatype0] HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[action] Oueries value: Queries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[type] Oueries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[guid] Oueries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[datatype0] Queries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[action] Queries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[type] HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[guid] Queries value: Queries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[datatype0] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[action] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[type] Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[guid] Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype0] Oueries value: Queries value: Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data1] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype2] HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data2] Queries value: Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype3] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[action] Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[type] Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[guid] Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype0] HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data0] Queries value: Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype1] Oueries value: $HKLM \ system \ current control set \ services \ browser \ trigger in fo \ 1 \ [data1]$ HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype2] Queries value: Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1ſdata21 Oueries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype3] HKLM\system\currentcontrolset\services\browser[imagepath] Oueries value: Queries value: HKLM\system\currentcontrolset\services\browser[type] Oueries value: HKLM\system\currentcontrolset\services\browser[start] Queries value: HKLM\system\currentcontrolset\services\browser[errorcontrol] Oueries value: HKLM\svstem\currentcontrolset\services\browser[tag] Oueries value: HKLM\system\currentcontrolset\services\browser[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\browser[dependongroup] Oueries value: HKLM\system\currentcontrolset\services\browser[group] Oueries value: HKLM\system\currentcontrolset\services\browser[objectname] Queries value: Oueries value: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[type] Queries value: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[guid] Oueries value: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[datatype0] Oueries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[action1 Oueries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[type] HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[guid] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[datatype0] Oueries value: Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache[imagepath] Oueries value: HKLM\system\currentcontrolset\services\dnscache[type] HKLM\system\currentcontrolset\services\dnscache[start] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache[errorcontrol] Oueries value: HKLM\system\currentcontrolset\services\dnscache[tag] Queries value: HKLM\system\currentcontrolset\services\dnscache[dependonservice] HKLM\system\currentcontrolset\services\dnscache[dependongroup] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache[group] Oueries value: HKLM\system\currentcontrolset\services\dnscache[objectname] Oueries value: HKLM\system\currentcontrolset\services\efs\triggerinfo\0[action] Oueries value: HKLM\system\currentcontrolset\services\efs\triggerinfo\0[type] Queries value: HKLM\system\currentcontrolset\services\efs\triggerinfo\0[guid] HKLM\system\currentcontrolset\services\efs\triggerinfo\0[datatype0] Oueries value: Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[action] Oueries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[type] Oueries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[guid] Oueries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[datatype0] Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[data0] Oueries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[datatype1]

HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[action]

```
Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[type]
                          HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[guid]
 Oueries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[datatype0]
 Queries value:
                          HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[data0]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[datatype1]
 Queries value:
                          HKLM\system\currentcontrolset\services\ikeext[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext[start]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext[errorcontrol]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext[tag]
                          HKLM\system\currentcontrolset\services\ikeext[dependonservice]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\ikeext[dependongroup]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext[group]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext[objectname]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[action]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[type]
 Oueries value:
                          HKLM\svstem\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]
 Queries value:
                          HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[guid]
 Queries 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]
 Queries value:
                          HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[guid]
                          HKLM \verb|\system| current controlset \verb|\services| lmhosts \verb|\triggerinfo| 1 [data type 0]
 Queries value:
 Queries value:
                          HKLM \setminus software \setminus microsoft \setminus sqmclient \setminus windows \setminus disabled processes \texttt{[a66e19e6]]}
 Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
 Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
                          HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[action]
 Queries value:
                          HKLM \setminus system \setminus current control set \setminus services \setminus policy agent \setminus trigger in fo \setminus 0 \texttt{[type]}
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[guid]
 Oueries value:
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype0]
                          HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[data0]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype1]
                          HKLM\system\currentcontrolset\services\policyagent[imagepath]
 Queries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\policyagent[type]
                          HKLM\system\currentcontrolset\services\policyagent[start]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\policyagent[errorcontrol]
 Oueries value:
                          HKLM\system\currentcontrolset\services\policyagent[tag]
 Oueries value:
                          HKLM\system\currentcontrolset\services\policyagent[dependonservice]
 Queries value:
                          HKLM\system\currentcontrolset\services\policyagent[dependongroup]
 Oueries value:
                          HKLM\system\currentcontrolset\services\policyagent[group]
 Queries value:
                          HKLM\system\currentcontrolset\services\policyagent[objectname]
 Oueries value:
                          HKLM\svstem\currentcontrolset\services\sensrsvc\triggerinfo\0[action]
 Oueries value:
                          HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[guid]
 Oueries value:
                          HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[datatype0]
 Oueries value:
                          HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[action]
 Queries value:
                          HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[guid]
 Queries value:
                          HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[datatype0]
 Oueries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[action]
 Oueries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[type]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus table tinput service \setminus trigger in fo \setminus 0 \ [guid]
 Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype0]
 Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data0]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data1]
 Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype2]
 Oueries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data2]
 Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype3]
 Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data3]
 Oueries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype4]
 Queries value:
                          HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[action]
```

HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[type]

HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[guid]

Oueries value:

```
Oueries value:
                                   HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[datatype0]
                                   HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[action]
  Oueries value:
  Oueries value:
                                   HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[type]
  Queries value:
                                   HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[guid]
  Oueries value:
                                   HKLM\svstem\currentcontrolset\services\w32time\triggerinfo\1\datatype01
  Queries 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]
  Oueries value:
HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[datatype0]
                                   HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[action]
  Oueries value:
  Queries value:
                                   HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[type]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[guid]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[datatype0]
  Oueries 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]
  Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[datatype0]
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[action]
  Queries value:
  Queries value:
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[type]
  Queries 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]
  Queries value:
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[type]
  Queries value:
  Queries value:
                                   HKLM \setminus system \setminus current control set \setminus services \setminus wpdbusenum \setminus triggerinfo \setminus 2 [guid]
  Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[datatype0]
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[action]
  Queries value:
  Queries value:
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[type]
  Queries value:
                                   Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[datatype0]
                                   HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[action]
  Oueries value:
  Queries value:
                                   HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[type]
  Queries value:
                                   HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[guid]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype0]
                                   HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[data0]
  Queries value:
  Queries value:
                                   HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype1]
                                   HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}[]
  Oueries value:
                                   HKCR\clsid\{660b90c8-73a9-4b58-8cae-
  Queries value:
355b7f55341b}\inprocserver32[inprocserver32]
                                  HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32[]
  Queries value:
                                   HKCR\clsid\{660b90c8-73a9-4b58-8cae-
  Oueries value:
355b7f55341b}\inprocserver32[threadingmodel]
                                  HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}[]
  Oueries value:
  Queries value:
                                  HKCR\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprocserver32[inprocserver32]
                                  HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprocserver32[]
  Queries value:
                                   HKCR\clsid\{a2a9545d-a0c2-42b4-9708-
  Oueries value:
a0b2badd77c8}\inprocserver32[threadingmodel]
                                  HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}[]
  Queries value:
                                  HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-
  Queries 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]
                                  HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}[]
  Oueries value:
                                  HKCR\clsid\{dd313e04-feff-11d1-8ecd-
  Queries value:
0000f87a470c}\inprocserver32[inprocserver32]
  Oueries value:
                                  HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32[]
                                   HKCR\clsid\{dd313e04-feff-11d1-8ecd-
  Queries value:
0000f87a470c}\inprocserver32[threadingmodel]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[programs]
  Queries value:
                                   HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common programs]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[favorites]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[{9e3995ab-1f9c-4f13-b827-48b24b6c7174}]
                                  HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Oueries value:
folders[{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
  Queries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ user as sist \ \{cebff5cd-ace2-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f78-4f78-4f78-4f78-4f78-
9926f41749ea}\count[{q65231o0-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]
  Oueries value:
                                  HKLM\system\currentcontrolset\services\dcomlaunch[objectname]
  Queries value:
                                   HKLM\system\currentcontrolset\services\rpceptmapper[objectname]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\rpcss[objectname]
```

HKLM\system\currentcontrolset\services\eventsystem[objectname]

```
Oueries value:
                         HKLM\system\currentcontrolset\services\bits[objectname]
                         HKLM\system\currentcontrolset\services\bits[imagepath]
 Oueries value:
 Oueries value:
                         HKLM\system\currentcontrolset\services\bits[requiredprivileges]
 Queries value:
                         HKLM\system\currentcontrolset\services\bits[type]
 Oueries value:
                         HKLM\system\currentcontrolset\services\bits[start]
 Queries value:
                         HKLM\system\currentcontrolset\services\bits[errorcontrol]
 Oueries value:
                         HKLM\system\currentcontrolset\services\bits[tag]
 Oueries value:
                         HKLM\system\currentcontrolset\services\bits[dependonservice]
 Oueries value:
                         HKLM\system\currentcontrolset\services\bits[dependongroup]
 Oueries value:
                         HKLM\system\currentcontrolset\services\bits[group]
 Oueries value:
                         HKLM\system\currentcontrolset\services\fontcache[objectname]
 Queries value:
                         HKLM\system\currentcontrolset\services\fontcache[imagepath]
 Oueries value:
                         HKLM\system\currentcontrolset\services\fontcache[requiredprivileges]
 Oueries value:
                         HKLM\system\currentcontrolset\services\http[objectname]
 Oueries value:
                         HKLM\system\currentcontrolset\services\ssdpsrv[objectname]
 Oueries value:
                         HKLM\system\currentcontrolset\services\ssdpsrv[imagepath]
                         HKLM\system\currentcontrolset\services\ssdpsrv[requiredprivileges]
 Oueries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\sppsvc[objectname]
 Oueries value:
                         HKLM\system\currentcontrolset\services\sppsvc[imagepath]
 Oueries value:
                         HKLM\system\currentcontrolset\services\sppsvc[requiredprivileges]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-
20[profileimagepath]
 Queries value:
                         shell folders[appdata]
 Queries value:
                         shell folders[local appdata]
 Queries value:
                         HKLM\system\currentcontrolset\services\sppsvc[environment]
 Queries value:
                         HKLM\system\currentcontrolset\control\mui\settings[preferreduilanguages]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\compatibility32[sppsvc]
 Queries value:
                         HKLM\system\currentcontrolset\control\wmi\security[bf3736e4-23ae-47c3-
b472-a03c2c3550fe]
                         Queries value:
9910-9b6fad873da7]
 Oueries value:
                         HKLM\system\currentcontrolset\control\wmi\security[e23b33b0-c8c9-472c-
a5f9-f2bdfea0f156]
                         HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
 Oueries value:
 Oueries value:
                         HKLM\software\microsoft\rpc\extensions[remoterpcdll]
 Queries value:
                         HKLM\software\microsoft\cryptography\defaults\provider types\type
001[name]
                         \label{lem:hklm} \verb+Kklm\+ software\+ icrosoft\+ cryptography\+ defaults\+ provider\+ microsoft\+ strong
 Queries value:
cryptographic provider[type]
                         HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
 Oueries value:
cryptographic provider[image path]
                         HKLM\system\currentcontrolset\control\wmi\security[0a592d4d-6d8e-403d-
 Oueries value:
9a4a-4d5e94dc5dc5]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wmpnetworksvc[objectname]
 Queries value:
                         HKLM\system\currentcontrolset\services\wmpnetworksvc[imagepath]
 Oueries value:
                         HKLM\svstem\currentcontrolset\services\wmpnetworksvc[requiredprivileges]
 Queries value:
                         HKLM\system\currentcontrolset\services\wmpnetworksvc[environment]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\compatibilitv32[wmpnetwk1
 Queries value:
                         HKLM\system\currentcontrolset\control\wmi\security[a7eb57f6-145e-4f18-
bd75-dbbf6f7e23a7]
                         HKLM\system\currentcontrolset\control\wmi\security[6a2dc7c1-930a-4fb5-
 Oueries value:
bb44-80b30aebed6c]
 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]
 Queries value:
                         HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
 Oueries value:
 Oueries value:
                         HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
                         HKLM\software\microsoft\windows\currentversion[devicepath]
 Oueries value:
 Queries value:
                         HKCR\clsid\{02e6ec4c-96e4-42e8-b533-336916a0087d}[]
 Oueries value:
                         HKCR\clsid\{02e6ec4c-96e4-42e8-b533-
336916a0087d}\inprocserver32[inprocserver32]
                         HKCR\clsid\{02e6ec4c-96e4-42e8-b533-336916a0087d}\inprocserver32[]
 Oueries value:
 Queries value:
                         HKCR\clsid\{02e6ec4c-96e4-42e8-b533-
336916a0087d}\inprocserver32[threadingmodel]
                        HKLM\software\microsoft\windows media player
 Oueries value:
nss\3.0[upnppingintervaloverrideinseconds]
 Queries value:
HKLM\system\currentcontrol\set\control\lsa\accessproviders[martaextension]
                         HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
 Queries value:
 Oueries value:
                         HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
 Oueries value:
                         HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
 Oueries value:
                         HKLM\software\microsoft\cryptography\rng[seed]
 Queries value:
                         HKLM\system\currentcontrolset\control\wmi\security[f404b94e-27e0-4384-
bfe8-1d8d390b0aa3]
```

Queries value: HKLM\system\currentcontrolset\control\wmi\security[bc97b970-d001-482f-

```
8745-b8d7d5759f99]
                 HKLM\software\microsoft\windows media foundation\platform[freewpptrace]
 Oueries value:
 Oueries value:
                 HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
                 HKLM\software\microsoft\drm[lastsessionid]
 Queries value:
                 Oueries value:
b9b8-05e4eca4977e]
 Oueries value:
                 HKLM\system\currentcontrolset\control\wmi\security[00000001-0dc9-401d-
b9b8-05e4eca4977e1
 Queries value:
                 HKLM\system\currentcontrolset\control\wmi\security[00000002-0dc9-401d-
b9b8-05e4eca4977e]
                 Oueries value:
b9b8-05e4eca4977e]
 Queries value:
                 HKLM\system\currentcontrolset\control\wmi\security[00000004-0dc9-401d-
b9b8-05e4eca4977e1
 Queries value:
                 HKLM\system\currentcontrolset\control\wmi\security[00000005-0dc9-401d-
b9b8-05e4eca4977e]
                 Queries value:
b9b8-05e4eca4977e]
 Queries value:
                 HKLM\system\currentcontrolset\services\crypt32[diaglevel]
 Oueries value:
                 HKLM\system\currentcontrolset\services\crypt32[diagmatchanymask]
 Queries value:
                 HKLM\system\currentcontrolset\services\cryptsvc[imagepath]
 Queries value:
                 HKLM\system\currentcontrolset\services\cryptsvc[type]
                 HKLM\system\currentcontrolset\services\cryptsvc[start]
 Oueries value:
 Queries value:
                 HKLM\system\currentcontrolset\services\cryptsvc[errorcontrol]
 Queries value:
                 HKLM\system\currentcontrolset\services\cryptsvc[tag]
 Oueries value:
                 {\tt HKLM \ } system \verb| current control set \verb| services \verb| cryptsvc[dependon service] 
 Queries value:
                 HKLM\system\currentcontrolset\services\cryptsvc[dependongroup]
 Queries value:
                 HKLM\system\currentcontrolset\services\cryptsvc[group]
 Oueries value:
                 HKLM\system\currentcontrolset\services\cryptsvc[objectname]
 Queries value:
                 HKLM\software\microsoft\drm[datapath]
 Queries value:
                 HKLM\software\microsoft\drm[upgradepath]
                 {\tt HKLM \setminus software \setminus microsoft \setminus ole[maximum allowed allocation size]}
 Queries value:
                 Queries value:
00-00-00]
                 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-
 Oueries value:
ca-8f-e01
 Queries value:
                 HKLM\software\microsoft\windows media player nss\3.0\devices\08-00-27-
ca-8f-e0[defaultauthorization]
 Oueries value:
9d55-7b8e7f157091}[category]
 Queries value:
9d55-7b8e7f157091}[name]
 Queries value:
9d55-7b8e7f157091}[parentfolder]
 Queries value:
9d55-7b8e7f157091}[description]
 Queries value:
9d55-7b8e7f157091}[relativepath]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[parsingname]
 Oueries value:
9d55-7b8e7f157091}[infotip]
 Oueries value:
9d55-7b8e7f157091}[localizedname]
 Oueries value:
9d55-7b8e7f157091}[icon]
 Queries value:
9d55-7b8e7f157091}[security]
 Queries value:
9d55-7b8e7f157091}[streamresource]
 Queries value:
9d55-7b8e7f157091}[streamresourcetype]
 Queries value:
9d55-7b8e7f157091}[localredirectonly]
 Oueries value:
```

9d55-7b8e7f157091}[roamable]

```
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[precreate]
    Oueries value:
9d55-7b8e7f157091}[stream1
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[publishexpandedpath]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[attributes]
    Queries value:
HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ 'f1b32785-6fba-4fcf-1000' and the software \ 'microsoft \ 'windows \ 'current version' \ 'explorer \ 'folder descriptions \ 'f1b32785-6fba-4fcf-1000' and the software \ 'microsoft \ 'windows \ 'current version' \ 'explorer \ 'folder descriptions \ 'f1b32785-6fba-4fcf-1000' and the software \ 'microsoft \ 'windows \ 'current version' \ 'explorer \ 'folder descriptions \ 'f1b32785-6fba-4fcf-1000' and the software \ 'windows \ 'explorer \ 'explorer \ 'f1b32785-6fba-4fcf-1000' and the software \ 'windows \
9d55-7b8e7f157091}[foldertypeid]
    Queries value:
9d55-7b8e7f157091}[initfolderhandler]
                                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
    Queries value:
folders[local appdata]
                                                                 HKLM\software\microsoft\windows media player nss\3.0\servers[0aef9a97-
    Queries value:
98cd-4f89-b183-3db737149306]
                                                                 HKLM\software\microsoft\windows media player nss\3.0\servers\0aef9a97-
    Queries value:
98cd-4f89-b183-3db737149306[defaultauthorization]
                                                                 HKLM\software\microsoft\windows media player nss\3.0\server settings\s-
    Queries value:
1-5-21-2160590473-689474908-1361669368-1002[0aef9a97-98cd-4f89-b183-3db737149306]
                                                                HKLM\software\microsoft\windows media player nss\3.0\events\{9360da4b-
    Queries value:
0822-41f5-a360-7f9b7a2e9449}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}[reason]
                                                                 HKLM\software\microsoft\windows media player nss\3.0\events\{9360da4b-
    Queries value:
0822-41f5-a360-7f9b7a2e9449}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}[id]
                                                                 HKLM\software\microsoft\windows media player nss\3.0\events\{9360da4b-
    Queries value:
0822-41f5-a360-7f9b7a2e9449}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}[data]
                                                                HKLM\software\microsoft\windows media player nss\3.0\events\{9360da4b-
    Queries value:
0822-41f5-a360-7f9b7a2e9449}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}[scope]
                                                                \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \software \verb|\microsoft| windows media player nss \verb|\scalebase| 3.0 \end{tabular} \end{tabular} \begin{tabular}{ll} All the lem of the l
    Queries value:
00-00-00[alive]
                                                                 HKLM\software\microsoft\windows media player nss\3.0\devices\08-00-27-
    Queries value:
ca-8f-e0[alive]
    Oueries value:
                                                                 HKLM\software\microsoft\com3[com+enabled]
                                                                 HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}\progid[]
    Queries value:
                                                                 HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}[]
    Queries value:
    Queries value:
                                                                HKCR\clsid\{e2085f28-feb7-404a-b8e7-
e659bdeaaa02}\inprocserver32[inprocserver32]
                                                                 HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}\inprocserver32[]
    Oueries value:
    Oueries value:
                                                                 HKCR\clsid\{e2085f28-feb7-404a-b8e7-
e659bdeaaa02}\inprocserver32[threadingmodel]
                                                                 HKLM\software\microsoft\ole[maxsxshashcount]
    Queries value:
                                                                 HKCR\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32[]
    Queries value:
    Queries value:
                                                                 HKLM\software\microsoft\rpc\extensions[ndroleextdll]
    Oueries value:
                                                                 HKLM\software\microsoft\sqmclient\windows\disabledprocesses[5512633]
    Queries value:
                                                                 HKLM\software\microsoft\com3[gipactivitybypass]
                                                                 HKCR\ interface \ \{adda3d55-6f72-4319-bff9-18600a539b10\}\ proxystubclsid32[]
    Oueries value:
                                                                 HKCR\clsid\{00020424-0000-0000-c000-00000000046}[]
    Oueries value:
    Queries value:
                                                                HKCR\clsid\{00020424-0000-0000-c000-
00000000046}\inprocserver32[inprocserver32]
                                                                 HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprocserver32[]
    Oueries value:
    Queries value:
                                                                 HKCR\clsid\{00020424-0000-0000-c000-
00000000046}\inprocserver32[threadingmodel]
                                                                 HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}\typelib[]
    Oueries value:
                                                                 HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}\typelib[version]
    Oueries value:
                                                                 HKCR\typelib\{db3442a7-a2e9-4a59-9cb5-f5c1a5d901e5}\1.0\0\win32[]
    Queries value:
    Queries value:
                                                                 HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32[]
    Oueries value:
                                                                 HKLM\software\microsoft\rpc[udtalignmentpolicy]
                                                                 HKCR\interface\{00020400-0000-0000-c000-00000000046}\proxystubclsid32[]
    Queries value:
                                                                 HKCR\clsid\{00020420-0000-0000-c000-00000000046}[]
    Oueries value:
    Oueries value:
                                                                 HKCR\clsid\{00020420-0000-0000-c000-
00000000046}\inprocserver32[inprocserver32]
                                                                 HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprocserver32[]
    Queries value:
    Oueries value:
                                                                 HKCR\clsid\{00020420-0000-0000-c000-
00000000046}\inprocserver32[threadingmodel]
                                                                 HKCR\interface\{e3bf6178-694e-459f-a5a6-191ea0ffa1c7}\proxystubclsid32[]
    Oueries value:
    Queries value:
                                                                 HKLM\software\microsoft\windows
\verb|nt\currentversion\software| protection platform \verb|plugins\modules\179b8a65-b0f6-41d9-acea-leady and the control of the con
12006ef9b32a[manifestfile]
    Queries value:
                                                                 HKLM\software\microsoft\windows
\verb|nt\currentversion\software| protection platform \verb|plugins\modules\179b8a65-b0f6-41d9-acea-leady and the control of the con
12006ef9b32a[pluginfile]
    Queries value:
                                                                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\modules\c42d83ff-5958-4af4-a0dd-
ba02fed39662[manifestfile]
    Oueries value:
                                                                 HKCR\interface\{e3bf6178-694e-459f-a5a6-191ea0ffa1c7}\typelib[]
    Queries value:
                                                                 HKCR \ interface \ \{e3bf6178-694e-459f-a5a6-191ea0ffa1c7\} \ typelib[version]
```

Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\modules\c42d83ff-5958-4af4-a0dd-

```
ba02fed39662[pluginfile]
                                                                     HKLM\software\microsoft\windows
    Oueries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/bios/4.0[moduleid]
    Queries value:
                                                                     HKLM\software\microsoft\windows
nt \verb|\currentversion\software protection platform \verb|\plugins\objects\msft:rm/algorithm/bios/4.0[is service]|
    Queries value:
                                                                     HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/flags/1.0[moduleid]
    Oueries value:
                                                                    HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/hwid/4.0[moduleid]
                                                                     HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/phone/1.0[moduleid]
                                                                     HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2005[moduleid]
    Oueries value:
                                                                    HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/vmd/1.0[moduleid]
                                                                     HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/volume/1.0[moduleid]
                                                                    HKLM\software\microsoft\windows
    Queries value:
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft:spp/licenseacquisition| payload handler/eul/1.0[moduleid]
    Queries value:
                                                                    HKLM\software\microsoft\windows
nt \verb|\colored | line 
                                                                     HKLM\software\microsoft\windows
    Queries value:
nt \verb|\currentversion| software protection platform \verb|\plugins| sobjects \verb|\msft:spp/licenseacquisition| payload handler/rac/1.0[moduleid]
                                                                     HKLM\software\microsoft\windows
    Queries value:
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft:spp/licenseacquisition/payload handler/spc/1.0[moduleid]|
    Queries value:
                                                                    HKLM\software\microsoft\windows
Queries value:
                                                                     HKLM\software\microsoft\windows
nt \verb|\currentversion| software protection platform \verb|\plugins| objects \verb|\msft:spp/taskscheduler/1.0[moduleid]| in the property of the prope
                                                                     HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/1.0[moduleid]
    Queries value:
                                                                    HKLM\software\microsoft\windows
\verb|nt\currentversion\software| protection platform \verb| plugins \verb| objects \verb| msft:spp/volume/services/kms/licenserenewal/1.0[moduleid]| | the province of the 
                                                                     HKLM\software\microsoft\windows
    Queries value:
nt \verb|\currentversion| software protection platform \verb|\plugins| objects \verb|\msft|: spp/windows functionality/agent/7.0[moduleid]| and the province of the property of the province of the property of the province of the prov
                                                                     HKCR \land [0405af4f-8b5c-447c-80f2-b75984a31f3c] \land [13c] \land [13c
    Queries value:
                                                                     HKCR\interface\{0405af4f-8b5c-447c-80f2-b75984a31f3c}\typelib[]
    Oueries value:
    Queries value:
                                                                     HKLM\software\microsoft\windows
nt \verb|\currentversion| software protection platform \verb|\plugins| objects \verb|\msft:spp/windowsfunctionality/agent/7.0[isservice]|
                                                                     Queries value:
    Sets/Creates value:
                                                                     HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-
409d6c4515e9}\inprocserver32[threadingmodel]
                                                                     HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-
    Sets/Creates value:
409d6c4515e9}\inprocserver32[]
    Sets/Creates value:
                                                                     HKLM\software\microsoft\windows media player nss\3.0\events\{6cc10660-
1516-4ed8-94f7-9cadbee645b1}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}[reason]
    Sets/Creates value:
                                                                     1516-4ed8-94f7-9cadbee645b1}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}[id]
                                                                     HKLM\software\microsoft\windows media player nss\3.0\events\{6cc10660-
    Sets/Creates value:
1516-4ed8-94f7-9cadbee645b1}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}[data]
    Sets/Creates value:
                                                                     HKLM\software\microsoft\windows media player nss\3.0\events\{6cc10660-
1516-4ed8-94f7-9cadbee645b1}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}[scope]
    Sets/Creates value:
                                                                     HKLM\software\microsoft\windows media player nss\3.0\events\{9360da4b-
0822-41f5-a360-7f9b7a2e9449}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}[reason]
    Sets/Creates value:
                                                                     HKLM\software\microsoft\windows media player nss\3.0\events\{9360da4b-
0822-41f5-a360-7f9b7a2e9449}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}[id]
    Sets/Creates value:
                                                                     HKLM\software\microsoft\windows media player nss\3.0\events\{9360da4b-
0822-41f5-a360-7f9b7a2e9449}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}[data]
    Sets/Creates value:
                                                                     HKLM\software\microsoft\windows media player nss\3.0\events\{9360da4b-
0822-41f5-a360-7f9b7a2e9449}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}[scope]
                                                                     HKCU\software\classes\local settings\muicache\27\52c64b7e[languagelist]
    Value changes:
    Value changes:
                                                                     HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\tinprocserver 32[]
    Value changes:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ set log\_entries \ 0000000000018 \ [packed catalog item]
    Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]
    Value changes:
Value changes:
Value changes:
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
    Value changes:
Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
```

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ catalog_entries \ 0000000000010 \ [packed catalog item]$

Value changes:

Value changes:

Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem] Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[packedcatalogitem]
Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem] Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000005[packedcatalogitem] Value changes:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem] Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem] Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[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\browser[start] Value changes: HKLM\system\currentcontrolset\services\policyagent[start]

Value changes:

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

9926f41749ea}\count[{q65231o0-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]

Value changes:

9926f41749ea}\count[hrzr_pgyfrffvba]

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

nss\3.0\servers[aliveservercount]