Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

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:	3331
Type:	basic
Owner:	admin
Label:	1be5bc13fd1cf615a95feec0c5b7fd13
Date Added:	2016-05-18 10:30:52 (UTC)
File Type:	PE32:win32:gui
File Size:	201728 bytes
MD5:	1be5bc13fd1cf615a95feec0c5b7fd13
SHA256:	10e3f54492e5cdcdf2c1ae6d097aafdea9474ff77bf6ccb5a9c762ccb6e4a347
Description:	None

Pattern Matching Results

7	Writes to memory of system processes
6	Modifies registry autorun entries
6	Writes to system32 folder
5	Abnormal sleep detected
7	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"]
Creates process:	C:\Windows\system32\cmd.exe ["C:\Windows\system32\cmd.exe"]
Creates process:	C:\Windows\system32\rundll32.exe [C:\Windows\system32\rundll32.exe bfe.dll,BfeOnServiceStartTypeChange]
Creates process:	C:\Windows\system32\sppsvc.exe [C:\Windows\system32\sppsvc.exe]
Creates process:	C:\Program Files\Windows Media Player\wmpnetwk.exe ["C:\Program Files\Windows Media Player\wmpnetwk.exe"]
Reads from process:	PID:2644 C:\Windows\System32\calc.exe
Writes to process:	PID:1184 C:\Windows\explorer.exe
Writes to process:	PID:456 C:\Windows\System32\services.exe
Writes to process:	PID:2600 C:\Windows\System32\cmd.exe
Terminates process:	C:\Windows\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe
Terminates process:	C:\Windows\System32\cmd.exe
Terminates process:	C:\Windows\System32\rundll32.exe
Creates remote thread:	C:\Windows\explorer.exe
Creates remote thread:	C:\Windows\System32\services.exe
Creates remote thread:	C:\Windows\System32\svchost.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\BaseNamedObjects\DBWinMutex
Creates event:	\BaseNamedObjects\Restricted\{0C5AB9CD-2F90-6754-8374-21D4DAB28CC1}
Creates event:	\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D78}
Creates event:	\BaseNamedObjects\SvcctrlStartEvent_A3752DX
Creates event:	\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D77}
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:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-1002
Creates:	C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-1002\$b136cea6dd8900e373425c26f869789d
Creates:	C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-1002\$b136cea6dd8900e373425c26f869789d\L
Creates:	C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-1002\$b136cea6dd8900e373425c26f869789d\U
Creates:	C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-1002\$b136cea6dd8900e373425c26f869789d\@

```
  Creates:                 C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-
1002\$b136cea6dd8900e373425c26f869789d\n
  Creates:                 C:\$Recycle.Bin\S-1-5-18
  Creates:                 C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d
  Creates:                 C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\L
  Creates:                 C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\U
  Creates:                 C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\@
  Creates:                 C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\n
  Creates:                 C:GAC_MSIL
  Creates:                 C:GAC
  Creates:                 C:\Windows\assembly\GAC\Desktop.ini
  Creates:                 C:\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
  Creates:
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player
NSS\3.0\SCPD
  Creates:
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player
NSS\3.0\Icon Files
  Opens:                   C:\Windows\Prefetch\1BE5BC13FD1CF615A95FEEC0C5B7F-CFDFB467.pf
  Opens:                   C:\Windows\System32
  Opens:                   C:\Windows\System32\sechost.dll
  Opens:                   C:\Windows\System32\imm32.dll
  Opens:                   C:includeincludeincludeincludeincludeinclude\
  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
  Opens:                   C:\Windows\MSWSOCK.dll
  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\@
  Opens:                   C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\U
  Opens:                   C:\Windows\System32\cmd.exe
  Opens:                   C:\Windows\System32\apphelp.dll
  Opens:                   C:\Windows\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe
  Opens:                   C:\Windows\Prefetch\CMD.EXE-4A81B364.pf
  Opens:                   C:
  Opens:                   C:\Program Files
  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
  Opens:                   C:\Windows\Branding\Basebrd\en-US
  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
  Opens:                   C:\Windows\System32\gdi32.dll
  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
  Opens:                   C:\Windows\System32\rundll32.exe
  Opens:                   C:\Windows\AppPatch\sysmain.sdb
  Opens:                  C:\Windows\Prefetch\RUNDLL32.EXE-39102DB5.pf
  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
  Opens:                  C:\Windows\ServiceProfiles
  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%4Operational.evtx
  Opens:                  C:\Windows\System32\RpcRtRemote.dll
  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
  Opens:                  C:\ProgramData\Microsoft\Network
  Opens:                  C:\ProgramData\Microsoft\Network\Downloader
  Opens:                  C:\ProgramData\Microsoft\Windows
  Opens:                  C:\ProgramData\Microsoft\Windows\DRM
  Opens:                  C:\Users
  Opens:                  C:\Users\Admin
  Opens:                  C:\Users\Admin\AppData
  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
  Opens:                  C:\Windows\Performance
  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
  Opens:                  C:\Windows\System32\provsvc.dll
  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
  Opens:                  C:\Windows\System32\ws2_32.dll
  Opens:                  C:\Windows\System32\nsi.dll
  Opens:                  C:\Windows\System32\IPHLPAPI.DLL
  Opens:                  C:\Windows\System32\winnsi.dll
  Opens:                  C:\Windows\System32\shlwapi.dll
  Opens:                  C:\Windows\System32\wtsapi32.dll
  Opens:                  C:\Program Files\Windows Media Player\en-US\wmpnetwk.exe.mui
  Opens:                        C:\Windows\System32\winsta.dll
  Opens:                        C:\Windows\System32\ntmarta.dll
  Opens:                        C:\Windows\System32\Wldap32.dll
  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
  Opens:                        C:\Windows\System32\en-US\setupapi.dll.mui
  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
  Opens:                        C:\ProgramData\Microsoft\Windows\DRM\blackbox.bin
  Opens:                        C:\ProgramData\Microsoft\Windows\DRM\v3ks.sec
  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
  Opens:                        C:\Windows\System32\sxs.dll
  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:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
  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
  Opens:                        C:\Users\Admin\AppData\Local\Microsoft\Media
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
  Opens:                        C:\Windows\System32\wship6.dll
  Opens:                        C:\Windows\System32\WinSATAPI.dll
  Opens:                        C:\Windows\System32\dxgi.dll
  Opens:                        C:\Windows\System32\en-US\WinSATAPI.dll.mui
  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\msxml3.dll
  Opens:                        C:\Windows\System32\msxml3r.dll
  Opens:                        C:\Windows\System32\dnsapi.dll
  Opens:                        C:\Windows\System32\urlmon.dll
  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
  Opens:                        C:\Windows\System32\powrprof.dll
  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
  Opens:                        C:\Windows\System32\charmap.exe
  Opens:                        C:\WINDOWS\PREFETCH\READYBOOT\TRACE1.FX
  Opens:                      C:\Windows\System32\SMI\Store\Machine\SCHEMA.DAT{e29ac73d-7037-11de-
816d-001c23e25b76}.TM.blf
  Opens:                      C:\Windows\System32\SMI\Store\Machine\SCHEMA.DAT
  Opens:                      C:\Windows\System32\en-US\FirewallAPI.dll.mui
  Opens:                      C:\Program Files\Windows Media Player\WSOCK32.dll
  Opens:                      C:\Program Files\Windows Media Player\IPHLPAPI.DLL
  Opens:                      C:\Program Files\Windows Media Player\WINNSI.DLL
  Opens:                      C:\Program Files\Windows Media Player\USERENV.dll
  Opens:                      C:\Program Files\Windows Media Player\profapi.dll
  Opens:                      C:\Program Files\Windows Media Player\WTSAPI32.dll
  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
  Opens:                      C:\Program Files\Windows Media Player\ntmarta.dll
  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:
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player NSS\3.0
  Opens:
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player NSS
  Opens:
C:\Windows\ServiceProfiles\NetworkService\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
  Opens:
C:\Windows\ServiceProfiles\NetworkService\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
  Opens:
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
  Opens:
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
  Opens:                      C:\Program Files\Windows Media Player\CRYPTSP.dll
  Opens:                      C:\Program Files\Windows Media Player\RpcRtRemote.dll
  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:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-
1002\$b136cea6dd8900e373425c26f869789d\@
  Writes to:                  C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-
1002\$b136cea6dd8900e373425c26f869789d\n
  Writes to:                  C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\@
  Writes to:                  C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\n
  Writes to:                  C:\Windows\assembly\GAC\Desktop.ini
  Writes to:                  C:\Windows\System32\LogFiles\Scm\5c2c622f-70e9-4194-a7da-033e827365ad
  Reads from:                 C:\Windows\Prefetch\CMD.EXE-4A81B364.pf
  Reads from:                 C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\@
  Reads from:                 C:\Windows\System32\LogFiles\Scm\5c2c622f-70e9-4194-a7da-033e827365ad
  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
  Reads from:                 C:\ProgramData\Microsoft\Windows\DRM\blackbox.bin
  Reads from:                 C:\ProgramData\Microsoft\Windows\DRM\v3ks.sec
  Reads from:                 C:\ProgramData\Microsoft\Windows\DRM\v3ks.bla
  Reads from:                 C:\Windows\System32\upnp.dll
  Reads from:                 C:\Windows\System32\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
```

Network Events

DNS query:	j.maxmind.com
DNS response:	j.maxmind.com ⇒ 127.0.0.1
Connects to:	127.0.0.1:80
Sends data to:	8.8.8.8:53
Sends data to:	83.133.123.20:53
Sends data to:	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:	80.109.74.3:16471
Sends data to:	130.204.226.4:16471
Sends data to:	221.244.148.250:16471
Sends data to:	176.227.128.250:16471
Sends data to:	173.80.73.5:16471
Sends data to:	74.210.157.7:16471
Sends data to:	180.47.189.7:16471
Sends data to:	74.56.221.248:16471
Sends data to:	37.192.19.8:16471
Sends data to:	68.119.104.8:16471
Sends data to:	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}\inprocserver32
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:	HKLM\software\microsoft\windows media player nss\3.0\events
Creates key:	HKLM\software\microsoft\windows media player nss\3.0\events\{9360da4b-0822-41f5-a360-7f9b7a2e9449}
Creates key:	HKLM\software\microsoft\cryptography\rng
Creates key:	HKLM\software\microsoft\windows media player nss\3.0\servers
Creates key:	HKLM\software\microsoft\windows media player nss\3.0\events\{6cc10660-1516-4ed8-94f7-9cadbee645b1}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}
Creates key:	HKLM\software\microsoft\windows media player nss\3.0\events\{9360da4b-0822-41f5-a360-7f9b7a2e9449}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}
Creates key:	HKLM\software\microsoft\windows media player nss\3.0\devices\00-00-00-

```
00-00-00
  Creates key:              HKLM\software\microsoft\windows media player nss\3.0\devices\08-00-27-
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\currentcontrolset\services\winsock2\parameters\appid_catalog
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\1e6c4482
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  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\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012
  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:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015
  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 key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
```

```
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
  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\system\currentcontrolset\services\winsock\parameters
  Opens key:                HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
  Opens key:                HKLM\system\currentcontrolset\services\psched\parameters\winsock
  Opens key:                HKLM\system\currentcontrolset\services\winsock\setup migration\providers
  Opens key:                HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
  Opens key:                HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
  Opens key:                HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
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
  Opens key:                HKLM\software\policies\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography\offload
  Opens key:                HKLM\software\microsoft\cryptography\deshashsessionkeybackward
  Opens key:                HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}\inprocserver32
  Opens key:                HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprocserver32
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{7007acc7-3202-11d1-
aad2-00805fc1270e}
  Opens key:                HKCU\software\classes\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}
  Opens key:                HKCR\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{21ec2020-3aea-1069-
a2dd-08002b30309d}
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\desktop\namespace\{21ec2020-3aea-1069-
a2dd-08002b30309d}
  Opens key:                HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}
  Opens key:                HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\controlpanel\namespace\{7007acc7-3202-
11d1-aad2-00805fc1270e}
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\controlpanel\namespace\{7007acc7-3202-
11d1-aad2-00805fc1270e}
  Opens key:                HKCU\software\classes\clsid\{2227a280-3aea-1069-a2de-08002b30309d}
  Opens key:                HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{2227a280-
3aea-1069-a2de-08002b30309d}
  Opens key:
HKCU\system\currentcontrolset\control\network\showwirelessconnectingonstart
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\controlpanel\namespace\namecustomizations
  Opens key:                HKLM\system\currentcontrolset\control\mui\stringcachesettings
  Opens key:                HKCU\software\classes\local settings\muicache\27\52c64b7e
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{7007acc7-
3202-11d1-aad2-00805fc1270e}
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\shellserviceobjects\{fd6905ce-952f-41f1-
9a6f-135d9c6622cc}
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\shellserviceobjects\{f56f6fdd-aa9d-4618-
a949-c1b91af43b1a}
  Opens key:                HKLM\software\microsoft\windows\currentversion\run
  Opens key:                HKLM\software\microsoft\rpc
  Opens key:                HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:                HKLM\system\setup
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                HKLM\system\currentcontrolset\control\sqmservicelist
  Opens key:                HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32
  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\currentcontrolset\control\session manager\environment
  Opens key:                HKLM\software\microsoft\windows\currentversion
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-18
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Opens key:                HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders
  Opens key:                HKU\.default\environment
  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
  Opens key:                HKLM\system\currentcontrolset\control\networkprovider\hworder
  Opens key:                HKLM\system\currentcontrolset\services\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:                HKLM\system\currentcontrolset\services\appinfo\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\appmgmt
  Opens key:                HKLM\system\currentcontrolset\services\appmgmt\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\audioendpointbuilder
  Opens key:                HKLM\system\currentcontrolset\services\audioendpointbuilder\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\audiosrv
  Opens key:                HKLM\system\currentcontrolset\services\audiosrv\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\axinstsv
  Opens key:                HKLM\system\currentcontrolset\services\axinstsv\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\bdesvc
  Opens key:                HKLM\system\currentcontrolset\services\bdesvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\bfe\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\bits
  Opens key:                HKLM\system\currentcontrolset\services\bits\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\browser
  Opens key:                HKLM\system\currentcontrolset\services\browser\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\browser\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\browser\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\browser\triggerinfo\2
  Opens key:                HKLM\system\currentcontrolset\services\bthserv
  Opens key:                HKLM\system\currentcontrolset\services\bthserv\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\bthserv\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\certpropsvc
  Opens key:                HKLM\system\currentcontrolset\services\certpropsvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32
  Opens key:
HKLM\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:                HKLM\system\currentcontrolset\services\defragsvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\dhcp
  Opens key:                HKLM\system\currentcontrolset\services\dhcp\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\dnscache
  Opens key:                HKLM\system\currentcontrolset\services\dnscache\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\dnscache\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\dot3svc
  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\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:                HKLM\system\currentcontrolset\services\keyiso\triggerinfo
  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\currentcontrolset\services\lanmanworkstation\triggerinfo
  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
Opens key:                HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1
Opens key:                HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2
Opens key:                HKLM\system\currentcontrolset\services\mcx2svc
Opens key:                HKLM\system\currentcontrolset\services\mcx2svc\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\mmcss
Opens key:                HKLM\system\currentcontrolset\services\mmcss\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\msdtc
Opens key:                HKLM\system\currentcontrolset\services\msdtc\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\msiscsi
Opens key:                HKLM\system\currentcontrolset\services\msiscsi\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\msiserver
Opens key:                HKLM\system\currentcontrolset\services\msiserver\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\napagent
Opens key:                HKLM\system\currentcontrolset\services\napagent\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\netlogon
Opens key:                HKLM\system\currentcontrolset\services\netlogon\triggerinfo
Opens key:                HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
Opens key:                HKLM\software\microsoft\sqmclient\windows\disabledsessions\
Opens key:                HKLM\system\currentcontrolset\services\netman
Opens key:                HKLM\system\currentcontrolset\services\netman\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\netprofm
Opens key:                HKLM\system\currentcontrolset\services\netprofm\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\nettcpportsharing
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
Opens key:                HKLM\system\currentcontrolset\services\ose
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
Opens key:                HKLM\system\currentcontrolset\services\pcasvc
Opens key:                HKLM\system\currentcontrolset\services\pcasvc\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\peerdistsvc
Opens key:                HKLM\system\currentcontrolset\services\peerdistsvc\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\pla
Opens key:                HKLM\system\currentcontrolset\services\pla\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\plugplay
Opens key:                HKLM\system\currentcontrolset\services\plugplay\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\pnrpautoreg
Opens key:                HKLM\system\currentcontrolset\services\pnrpautoreg\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\pnrpsvc
Opens key:                HKLM\system\currentcontrolset\services\pnrpsvc\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\policyagent
Opens key:                HKLM\system\currentcontrolset\services\policyagent\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0
Opens key:                HKLM\system\currentcontrolset\services\policyagent\triggerinfo\1
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 key:                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
Opens key:                HKLM\system\currentcontrolset\services\rasauto
Opens key:                HKLM\system\currentcontrolset\services\rasauto\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\rasman
Opens key:                HKLM\system\currentcontrolset\services\rasman\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\remoteaccess
Opens key:                HKLM\system\currentcontrolset\services\remoteaccess\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\remoteregistry
Opens key:                HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\rpceptmapper
Opens key:                HKLM\system\currentcontrolset\services\rpceptmapper\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\rpclocator
Opens key:                HKLM\system\currentcontrolset\services\rpclocator\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\rpcss
Opens key:                HKLM\system\currentcontrolset\services\rpcss\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\samss
Opens key:                HKLM\system\currentcontrolset\services\samss\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\scardsvr
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
Opens key:              HKLM\system\currentcontrolset\services\seclogon\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\sens
Opens key:              HKLM\system\currentcontrolset\services\sens\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\sensrsvc
Opens key:              HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0
Opens key:              HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1
Opens key:              HKLM\system\currentcontrolset\services\sessionenv
Opens key:              HKLM\system\currentcontrolset\services\sessionenv\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\shellhwdetection
Opens key:              HKLM\system\currentcontrolset\services\shellhwdetection\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\snmptrap
Opens key:              HKLM\system\currentcontrolset\services\snmptrap\triggerinfo
Opens key:              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 key:              HKLM\system\currentcontrolset\services\sppuinotify
Opens key:              HKLM\system\currentcontrolset\services\sppuinotify\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\ssdpsrv
Opens key:              HKLM\system\currentcontrolset\services\ssdpsrv\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\sstpsvc
Opens key:              HKLM\system\currentcontrolset\services\sstpsvc\triggerinfo
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
Opens key:              HKLM\system\currentcontrolset\services\storsvc\triggerinfo\1
Opens key:              HKLM\system\currentcontrolset\services\swprv
Opens key:              HKLM\system\currentcontrolset\services\swprv\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\sysmain
Opens key:              HKLM\system\currentcontrolset\services\sysmain\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\tabletinputservice
Opens key:              HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0
Opens key:              HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\1
Opens key:              HKLM\system\currentcontrolset\services\tapisrv
Opens key:              HKLM\system\currentcontrolset\services\tapisrv\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\tbs
Opens key:              HKLM\system\currentcontrolset\services\tbs\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\termservice
Opens key:              HKLM\system\currentcontrolset\services\termservice\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\themes
Opens key:              HKLM\system\currentcontrolset\services\themes\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\threadorder
Opens key:              HKLM\system\currentcontrolset\services\threadorder\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\tlntsvr
Opens key:              HKLM\system\currentcontrolset\services\tlntsvr\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\trkwks
Opens key:              HKLM\system\currentcontrolset\services\trkwks\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\trustedinstaller
Opens key:              HKLM\system\currentcontrolset\services\trustedinstaller\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\ui0detect
Opens key:              HKLM\system\currentcontrolset\services\ui0detect\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\umrdpservice
Opens key:              HKLM\system\currentcontrolset\services\umrdpservice\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\upnphost
Opens key:              HKLM\system\currentcontrolset\services\upnphost\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\uxsms
Opens key:              HKLM\system\currentcontrolset\services\uxsms\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\vaultsvc
Opens key:              HKLM\system\currentcontrolset\services\vaultsvc\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\vds
Opens key:              HKLM\system\currentcontrolset\services\vds\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\vss
Opens key:              HKLM\system\currentcontrolset\services\vss\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\w32time
Opens key:              HKLM\system\currentcontrolset\services\w32time\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\w32time\triggerinfo\0
Opens key:              HKLM\system\currentcontrolset\services\w32time\triggerinfo\1
Opens key:              HKLM\system\currentcontrolset\services\w32time\triggerinfo\2
Opens key:              HKLM\system\currentcontrolset\services\wbengine
Opens key:              HKLM\system\currentcontrolset\services\wbengine\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\wbiosrvc
Opens key:              HKLM\system\currentcontrolset\services\wbiosrvc\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\wcncsvc
Opens key:              HKLM\system\currentcontrolset\services\wcncsvc\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\wcspluginservice
Opens key:              HKLM\system\currentcontrolset\services\wcspluginservice\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\wdiservicehost
Opens key:              HKLM\system\currentcontrolset\services\wdiservicehost\triggerinfo
Opens key:              HKLM\system\currentcontrolset\services\wdisystemhost
```

```
  Opens key:                HKLM\system\currentcontrolset\services\wdisystemhost\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\webclient
  Opens key:                HKLM\system\currentcontrolset\services\webclient\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\webclient\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\webclient\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\wecsvc
  Opens key:                HKLM\system\currentcontrolset\services\wecsvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\wercplsupport
  Opens key:                HKLM\system\currentcontrolset\services\wercplsupport\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\wersvc
  Opens key:                HKLM\system\currentcontrolset\services\wersvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\wersvc\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\winhttpautoproxysvc
  Opens key:                HKLM\system\currentcontrolset\services\winhttpautoproxysvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\winmgmt
  Opens key:                HKLM\system\currentcontrolset\services\winmgmt\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\winrm
  Opens key:                HKLM\system\currentcontrolset\services\winrm\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\wlansvc
  Opens key:                HKLM\system\currentcontrolset\services\wlansvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\wmiapsrv
  Opens key:                HKLM\system\currentcontrolset\services\wmiapsrv\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\wmpnetworksvc
  Opens key:                HKLM\system\currentcontrolset\services\wmpnetworksvc\triggerinfo
  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\system\currentcontrolset\services\wpdbusenum\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2
  Opens key:                HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3
  Opens key:                HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4
  Opens key:                HKLM\system\currentcontrolset\services\wsearch
  Opens key:                HKLM\system\currentcontrolset\services\wsearch\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\wuauserv
  Opens key:                HKLM\system\currentcontrolset\services\wuauserv\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\wudfsvc
  Opens key:                HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\wwansvc
  Opens key:                HKLM\system\currentcontrolset\services\wwansvc\triggerinfo
  Opens key:                HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
  Opens key:                HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
  Opens key:                HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\treatas
  Opens key:                HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\treatas
  Opens key:                HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\progid
  Opens key:                HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\progid
  Opens key:                HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\inprocserver32
  Opens key:                HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\inprochandler32
  Opens key:                HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\inprochandler
  Opens key:                HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler
  Opens key:                HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}
  Opens key:                HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}
  Opens key:                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
  Opens key:                HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprochandler
  Opens key:                HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprochandler
  Opens key:                HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}
  Opens key:                HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}
  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
  Opens key:                HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\progid
  Opens key:                HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-
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:                HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\treatas
  Opens key:                HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\progid
  Opens key:                HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\progid
  Opens key:                HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\inprocserver32
  Opens key:                HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\inprochandler32
  Opens key:                HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\inprochandler
  Opens key:                HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprochandler
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
  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
nt\currentversion\softwareprotectionplatform
  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\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}\treatas
  Opens key:                HKCR\clsid\{02e6ec4c-96e4-42e8-b533-336916a0087d}\progid
  Opens key:                HKCR\clsid\{02e6ec4c-96e4-42e8-b533-336916a0087d}\inprocserver32
  Opens key:                HKCR\clsid\{02e6ec4c-96e4-42e8-b533-336916a0087d}\inprochandler32
  Opens key:                HKCR\clsid\{02e6ec4c-96e4-42e8-b533-336916a0087d}\inprochandler
  Opens key:                HKLM\system\currentcontrolset\control\lsa\accessproviders
  Opens key:                 HKLM\system\currentcontrolset\services\ldap
  Opens key:                 HKLM\software\microsoft\windows media foundation\platform
  Opens key:                 HKLM\system\currentcontrolset\services\crypt32
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\msasn1
  Opens key:                 HKLM\software\microsoft\drm
  Opens key:                 HKLM\software\microsoft\cryptography\oid
  Opens key:                 HKLM\software\microsoft\cryptography\oid\encodingtype 0
  Opens key:                 HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdlldecodeobjectex
  Opens key:                 HKLM\software\microsoft\cryptography\oid\encodingtype 1
  Opens key:                 HKLM\software\microsoft\cryptography\oid\encodingtype
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
  Opens key:                 HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.11
  Opens key:                 HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.12
  Opens key:                 HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.2
  Opens key:                 HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.3
  Opens key:                 HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.4
  Opens key:                 HKLM\software\microsoft\windows media player nss\3.0\mac access control
  Opens key:                 HKLM\software\microsoft\windows media player nss\3.0\devices\00-00-00-
00-00-00
  Opens key:                 HKLM\software\microsoft\windows media player nss\3.0\devices\08-00-27-
ca-8f-e0
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
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
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\0
  Opens key:                 HKCU\control panel\international
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings
  Opens key:                 HKLM\software\microsoft\windows media player nss\3.0\server settings
  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
  Opens key:                 HKLM\software\microsoft\windows media player nss\3.0\events\{6cc10660-
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}
  Opens key:                 HKLM\software\microsoft\windows media player nss\3.0\events\{9360da4b-
0822-41f5-a360-7f9b7a2e9449}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}
  Opens key:                 HKLM\software\microsoft\com3
  Opens key:                 HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}
  Opens key:                 HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}\treatas
  Opens key:                 HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}\progid
  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-c000-000000000046}
  Opens key:                 HKCR\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
  Opens key:                 HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}
  Opens key:                 HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}\proxystubclsid32
  Opens key:                 HKCR\clsid\{00020424-0000-0000-c000-000000000046}
  Opens key:                 HKCR\clsid\{00020424-0000-0000-c000-000000000046}\treatas
  Opens key:                 HKCR\clsid\{00020424-0000-0000-c000-000000000046}\progid
  Opens key:                 HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32
  Opens key:                 HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprochandler32
  Opens key:                 HKCR\clsid\{00020424-0000-0000-c000-000000000046}\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}
  Opens key:                 HKCR\typelib\{db3442a7-a2e9-4a59-9cb5-f5c1a5d901e5}\1.0
  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
  Opens key:                 HKCR\typelib\{00020430-0000-0000-c000-000000000046}
  Opens key:                 HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0
  Opens key:                 HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0
  Opens key:                 HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32
  Opens key:              HKCR\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:              HKCR\interface\{00020400-0000-0000-c000-000000000046}\proxystubclsid32
  Opens key:              HKCR\clsid\{00020420-0000-0000-c000-000000000046}
  Opens key:              HKCR\clsid\{00020420-0000-0000-c000-000000000046}\treatas
  Opens key:              HKCR\clsid\{00020420-0000-0000-c000-000000000046}\progid
  Opens key:              HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32
  Opens key:              HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprochandler32
  Opens key:              HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprochandler
  Opens key:              HKCR\interface\{e3bf6178-694e-459f-a5a6-191ea0ffa1c7}
  Opens key:              HKCR\interface\{e3bf6178-694e-459f-a5a6-191ea0ffa1c7}\proxystubclsid32
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\modules
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\modules\179b8a65-b0f6-41d9-acea-12006ef9b32a
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\modules\c42d83ff-5958-4af4-a0dd-ba02fed39662
  Opens key:              HKCR\interface\{e3bf6178-694e-459f-a5a6-191ea0ffa1c7}\forward
  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
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/flags/1.0
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/hwid/4.0
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/phone/1.0
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2005
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/vmd/1.0
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/volume/1.0
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/eul/1.0
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pkc/1.0
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/rac/1.0
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/spc/1.0
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/sequence/1.0
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/taskscheduler/1.0
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/1.0
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/licenserenewal/1.0
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/windowsfunctionality/agent/7.0
  Opens key:              HKCR\interface\{0405af4f-8b5c-447c-80f2-b75984a31f3c}
  Opens key:              HKCR\interface\{0405af4f-8b5c-447c-80f2-b75984a31f3c}\proxystubclsid32
  Opens key:              HKCR\interface\{0405af4f-8b5c-447c-80f2-b75984a31f3c}\forward
  Opens key:              HKCR\interface\{0405af4f-8b5c-447c-80f2-b75984a31f3c}\typelib
  Queries value:          HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
  Queries value:          HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:          HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:          HKCU\control panel\desktop[preferreduilanguages]
  Queries value:          HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Queries value:          HKLM\system\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]
  Queries value:          HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Queries value:          HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
```

```
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[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\000000000005[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
   Queries value:             HKLM\system\currentcontrolset\services\winsock\parameters[transports]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
   Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping]
   Queries value:             HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched[winsock 2.0 provider id]
   Queries value:             HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
   Queries value:             HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
```

```
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
  Queries value:            HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0[type]
  Queries value:            HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0[image path]
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries value:            HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  Queries value:            HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
  Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
  Queries value:            HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
  Queries value:            HKLM\software\microsoft\cryptography[machineguid]
  Queries value:            HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprocserver32[]
  Queries value:            HKCR\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}\inprocserver32[loadwithoutcom]
  Queries value:            HKCR\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}[sortorderindex]
  Queries value:            HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[sortorderindex]
  Queries value:            HKCR\clsid\{2227a280-3aea-1069-a2de-
08002b30309d}[system.itemnamedisplay]
  Queries value:            HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}[{b725f130-47ef-101a-
a5f1-02608c9eebac} 10]
  Queries value:            HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}[localizedstring]
  Queries value:
HKLM\system\currentcontrolset\control\mui\stringcachesettings[stringcachegeneration]
  Queries value:            HKCU\software\classes\local
settings\muicache\27\52c64b7e[@c:\windows\system32\prnfldr.dll,-8036]
  Queries value:            HKCR\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}[system.itemnamedisplay]
  Queries value:            HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[{b725f130-47ef-101a-
a5f1-02608c9eebac} 10]
  Queries value:            HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[localizedstring]
  Queries value:            HKCU\software\classes\local
settings\muicache\27\52c64b7e[@c:\windows\system32\netshell.dll,-1200]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[n]
  Queries value:            HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:            HKLM\system\setup[oobeinprogress]
  Queries value:            HKLM\system\setup[systemsetupinprogress]
  Queries value:            HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[current_protocol_catalog]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[current_namespace_catalog]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disablelocaloverride]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\compatibility32[cmd]
  Queries value:            HKLM\system\currentcontrolset\control\cmf\config[system]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist[public]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist[default]
  Queries value:            HKLM\software\microsoft\windows\currentversion[programfilesdir]
  Queries value:            HKLM\software\microsoft\windows\currentversion[commonfilesdir]
  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]
  Queries value:            HKLM\software\microsoft\windows\currentversion[commonw6432dir]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-
18[profileimagepath]
  Queries value:            HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[appdata]
  Queries value:            HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[local appdata]
  Queries value:            HKU\.default\control panel\desktop[preferreduilanguages]
  Queries value:            HKU\.default\control
panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\compatibility32[rundll32]
```

```
  Queries value:              HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:              HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:              HKLM\system\currentcontrolset\services\bfe[imagepath]
  Queries value:              HKLM\system\currentcontrolset\services\bfe[type]
  Queries value:              HKLM\system\currentcontrolset\services\bfe[start]
  Queries value:              HKLM\system\currentcontrolset\services\bfe[errorcontrol]
  Queries value:              HKLM\system\currentcontrolset\services\bfe[tag]
  Queries value:              HKLM\system\currentcontrolset\services\bfe[dependonservice]
  Queries value:              HKLM\system\currentcontrolset\services\bfe[dependongroup]
  Queries value:              HKLM\system\currentcontrolset\services\bfe[group]
  Queries value:              HKLM\system\currentcontrolset\services\bfe[objectname]
  Queries value:              HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[guid]
  Queries value:
HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[guid]
  Queries value:              HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[guid]
  Queries value:              HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\browser\triggerinfo\0[action]
  Queries 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]
  Queries value:              HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data0]
  Queries value:              HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype1]
  Queries value:              HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data1]
  Queries value:              HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype2]
  Queries value:              HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data2]
  Queries value:              HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype3]
  Queries 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]
  Queries value:              HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data0]
  Queries value:              HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype1]
  Queries value:              HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data1]
  Queries value:              HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype2]
  Queries value:              HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data2]
  Queries value:              HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype3]
  Queries value:              HKLM\system\currentcontrolset\services\browser[imagepath]
  Queries value:              HKLM\system\currentcontrolset\services\browser[type]
  Queries value:              HKLM\system\currentcontrolset\services\browser[start]
  Queries value:              HKLM\system\currentcontrolset\services\browser[errorcontrol]
  Queries value:              HKLM\system\currentcontrolset\services\browser[tag]
  Queries value:              HKLM\system\currentcontrolset\services\browser[dependonservice]
  Queries value:              HKLM\system\currentcontrolset\services\browser[dependongroup]
  Queries value:              HKLM\system\currentcontrolset\services\browser[group]
  Queries value:              HKLM\system\currentcontrolset\services\browser[objectname]
  Queries value:              HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[guid]
  Queries value:              HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[guid]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[data0]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[datatype1]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache[imagepath]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache[type]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache[start]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache[errorcontrol]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache[tag]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache[dependonservice]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache[dependongroup]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache[group]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache[objectname]
  Queries value:              HKLM\system\currentcontrolset\services\efs\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\efs\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\efs\triggerinfo\0[guid]
  Queries value:              HKLM\system\currentcontrolset\services\efs\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[guid]
  Queries value:              HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[data0]
  Queries value:              HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[datatype1]
  Queries value:              HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[guid]
  Queries value:              HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[data0]
  Queries value:              HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[datatype1]
  Queries value:              HKLM\system\currentcontrolset\services\ikeext[imagepath]
  Queries value:              HKLM\system\currentcontrolset\services\ikeext[type]
  Queries value:              HKLM\system\currentcontrolset\services\ikeext[start]
  Queries value:              HKLM\system\currentcontrolset\services\ikeext[errorcontrol]
  Queries value:              HKLM\system\currentcontrolset\services\ikeext[tag]
  Queries value:              HKLM\system\currentcontrolset\services\ikeext[dependonservice]
  Queries value:              HKLM\system\currentcontrolset\services\ikeext[dependongroup]
  Queries value:              HKLM\system\currentcontrolset\services\ikeext[group]
  Queries value:              HKLM\system\currentcontrolset\services\ikeext[objectname]
  Queries value:              HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[guid]
  Queries value:              HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[action]
  Queries 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]
  Queries 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]
  Queries value:              HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[datatype0]
  Queries value:              HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a66e19e6]
  Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
  Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
  Queries value:              HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[guid]
  Queries value:
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[data0]
  Queries value:
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype1]
  Queries value:              HKLM\system\currentcontrolset\services\policyagent[imagepath]
  Queries value:              HKLM\system\currentcontrolset\services\policyagent[type]
  Queries value:              HKLM\system\currentcontrolset\services\policyagent[start]
  Queries value:              HKLM\system\currentcontrolset\services\policyagent[errorcontrol]
  Queries value:              HKLM\system\currentcontrolset\services\policyagent[tag]
  Queries value:              HKLM\system\currentcontrolset\services\policyagent[dependonservice]
  Queries value:              HKLM\system\currentcontrolset\services\policyagent[dependongroup]
  Queries value:              HKLM\system\currentcontrolset\services\policyagent[group]
  Queries value:              HKLM\system\currentcontrolset\services\policyagent[objectname]
  Queries value:              HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[guid]
  Queries value:              HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[guid]
  Queries value:              HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[datatype0]
  Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[action]
  Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[type]
  Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[guid]
  Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype0]
  Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data0]
  Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype1]
  Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data1]
  Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype2]
  Queries 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]
  Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype4]
  Queries value:              HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[guid]
  Queries value:              HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[action]
  Queries value:              HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[type]
  Queries value:              HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[guid]
  Queries value:              HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[guid]
  Queries value:
HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[guid]
  Queries value:              HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[guid]
  Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[action]
  Queries value:              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[type]
  Queries value:              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[guid]
  Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[action]
  Queries value:              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[type]
  Queries value:              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[guid]
  Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[action]
  Queries value:              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[type]
  Queries value:              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[guid]
  Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[guid]
  Queries value:              HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[data0]
  Queries value:              HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype1]
  Queries value:              HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}[]
  Queries value:              HKCR\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32[]
  Queries value:              HKCR\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\inprocserver32[threadingmodel]
  Queries value:              HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}[]
  Queries value:              HKCR\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprocserver32[]
  Queries value:              HKCR\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprocserver32[threadingmodel]
  Queries value:              HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}[]
  Queries value:              HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-
535773d48449}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprocserver32[]
  Queries value:              HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-
535773d48449}\inprocserver32[threadingmodel]
  Queries value:              HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}[]
  Queries value:              HKCR\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32[]
  Queries value:              HKCR\clsid\{dd313e04-feff-11d1-8ecd-
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}]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-
9926f41749ea}\count[{q65231o0-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]
  Queries value:              HKLM\system\currentcontrolset\services\dcomlaunch[objectname]
  Queries value:              HKLM\system\currentcontrolset\services\rpceptmapper[objectname]
  Queries value:              HKLM\system\currentcontrolset\services\rpcss[objectname]
  Queries value:              HKLM\system\currentcontrolset\services\eventsystem[objectname]
  Queries value:            HKLM\system\currentcontrolset\services\bits[objectname]
  Queries value:            HKLM\system\currentcontrolset\services\bits[imagepath]
  Queries value:            HKLM\system\currentcontrolset\services\bits[requiredprivileges]
  Queries value:            HKLM\system\currentcontrolset\services\bits[type]
  Queries value:            HKLM\system\currentcontrolset\services\bits[start]
  Queries value:            HKLM\system\currentcontrolset\services\bits[errorcontrol]
  Queries value:            HKLM\system\currentcontrolset\services\bits[tag]
  Queries value:            HKLM\system\currentcontrolset\services\bits[dependonservice]
  Queries value:            HKLM\system\currentcontrolset\services\bits[dependongroup]
  Queries value:            HKLM\system\currentcontrolset\services\bits[group]
  Queries value:            HKLM\system\currentcontrolset\services\fontcache[objectname]
  Queries value:            HKLM\system\currentcontrolset\services\fontcache[imagepath]
  Queries value:            HKLM\system\currentcontrolset\services\fontcache[requiredprivileges]
  Queries value:            HKLM\system\currentcontrolset\services\http[objectname]
  Queries value:            HKLM\system\currentcontrolset\services\ssdpsrv[objectname]
  Queries value:            HKLM\system\currentcontrolset\services\ssdpsrv[imagepath]
  Queries value:            HKLM\system\currentcontrolset\services\ssdpsrv[requiredprivileges]
  Queries value:            HKLM\system\currentcontrolset\services\sppsvc[objectname]
  Queries value:            HKLM\system\currentcontrolset\services\sppsvc[imagepath]
  Queries value:            HKLM\system\currentcontrolset\services\sppsvc[requiredprivileges]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-
20[profileimagepath]
  Queries value:            HKU\s-1-5-20\software\microsoft\windows\currentversion\explorer\user
shell folders[appdata]
  Queries value:            HKU\s-1-5-20\software\microsoft\windows\currentversion\explorer\user
shell folders[local appdata]
  Queries value:            HKLM\system\currentcontrolset\services\sppsvc[environment]
  Queries value:            HKLM\system\currentcontrolset\control\mui\settings[preferreduilanguages]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\compatibility32[sppsvc]
  Queries value:            HKLM\system\currentcontrolset\control\wmi\security[bf3736e4-23ae-47c3-
b472-a03c2c3550fe]
  Queries value:            HKLM\system\currentcontrolset\control\wmi\security[5b6189d4-c1fd-4a8c-
9910-9b6fad873da7]
  Queries value:            HKLM\system\currentcontrolset\control\wmi\security[e23b33b0-c8c9-472c-
a5f9-f2bdfea0f156]
  Queries value:            HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Queries value:            HKLM\software\microsoft\rpc\extensions[remoterpcdll]
  Queries value:            HKLM\software\microsoft\cryptography\defaults\provider types\type
001[name]
  Queries value:            HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
  Queries value:            HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
  Queries value:            HKLM\system\currentcontrolset\control\wmi\security[0a592d4d-6d8e-403d-
9a4a-4d5e94dc5dc5]
  Queries value:            HKLM\system\currentcontrolset\services\wmpnetworksvc[objectname]
  Queries value:            HKLM\system\currentcontrolset\services\wmpnetworksvc[imagepath]
  Queries value:            HKLM\system\currentcontrolset\services\wmpnetworksvc[requiredprivileges]
  Queries value:            HKLM\system\currentcontrolset\services\wmpnetworksvc[environment]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\compatibility32[wmpnetwk]
  Queries value:            HKLM\system\currentcontrolset\control\wmi\security[a7eb57f6-145e-4f18-
bd75-dbbf6f7e23a7]
  Queries value:            HKLM\system\currentcontrolset\control\wmi\security[6a2dc7c1-930a-4fb5-
bb44-80b30aebed6c]
  Queries 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]
  Queries value:            HKLM\software\microsoft\windows media player nss\3.0[enabledlnatags]
  Queries value:            HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
  Queries value:            HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
  Queries value:            HKLM\software\microsoft\windows\currentversion[devicepath]
  Queries value:            HKCR\clsid\{02e6ec4c-96e4-42e8-b533-336916a0087d}[]
  Queries value:            HKCR\clsid\{02e6ec4c-96e4-42e8-b533-
336916a0087d}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{02e6ec4c-96e4-42e8-b533-336916a0087d}\inprocserver32[]
  Queries value:            HKCR\clsid\{02e6ec4c-96e4-42e8-b533-
336916a0087d}\inprocserver32[threadingmodel]
  Queries value:            HKLM\software\microsoft\windows media player
nss\3.0[upnppingintervaloverrideinseconds]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
  Queries value:            HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
  Queries value:            HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
  Queries value:            HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
  Queries 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]
   Queries value:            HKLM\software\microsoft\windows media foundation\platform[freewpptrace]
   Queries value:            HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
   Queries value:            HKLM\software\microsoft\drm[lastsessionid]
   Queries value:            HKLM\system\currentcontrolset\control\wmi\security[00000000-0dc9-401d-
b9b8-05e4eca4977e]
   Queries value:            HKLM\system\currentcontrolset\control\wmi\security[00000001-0dc9-401d-
b9b8-05e4eca4977e]
   Queries value:            HKLM\system\currentcontrolset\control\wmi\security[00000002-0dc9-401d-
b9b8-05e4eca4977e]
   Queries value:            HKLM\system\currentcontrolset\control\wmi\security[00000003-0dc9-401d-
b9b8-05e4eca4977e]
   Queries value:            HKLM\system\currentcontrolset\control\wmi\security[00000004-0dc9-401d-
b9b8-05e4eca4977e]
   Queries value:            HKLM\system\currentcontrolset\control\wmi\security[00000005-0dc9-401d-
b9b8-05e4eca4977e]
   Queries value:            HKLM\system\currentcontrolset\control\wmi\security[00000006-0dc9-401d-
b9b8-05e4eca4977e]
   Queries value:            HKLM\system\currentcontrolset\services\crypt32[diaglevel]
   Queries value:            HKLM\system\currentcontrolset\services\crypt32[diagmatchanymask]
   Queries value:            HKLM\system\currentcontrolset\services\cryptsvc[imagepath]
   Queries value:            HKLM\system\currentcontrolset\services\cryptsvc[type]
   Queries value:            HKLM\system\currentcontrolset\services\cryptsvc[start]
   Queries value:            HKLM\system\currentcontrolset\services\cryptsvc[errorcontrol]
   Queries value:            HKLM\system\currentcontrolset\services\cryptsvc[tag]
   Queries value:            HKLM\system\currentcontrolset\services\cryptsvc[dependonservice]
   Queries value:            HKLM\system\currentcontrolset\services\cryptsvc[dependongroup]
   Queries value:            HKLM\system\currentcontrolset\services\cryptsvc[group]
   Queries value:            HKLM\system\currentcontrolset\services\cryptsvc[objectname]
   Queries value:            HKLM\software\microsoft\drm[datapath]
   Queries value:            HKLM\software\microsoft\drm[upgradepath]
   Queries value:            HKLM\software\microsoft\ole[maximumallowedallocationsize]
   Queries value:            HKLM\software\microsoft\windows media player nss\3.0\devices[00-00-00-
00-00-00]
   Queries value:            HKLM\software\microsoft\windows media player nss\3.0\devices\00-00-00-
00-00-00[defaultauthorization]
   Queries value:            HKLM\software\microsoft\windows media player nss\3.0\devices[08-00-27-
ca-8f-e0]
   Queries value:            HKLM\software\microsoft\windows media player nss\3.0\devices\08-00-27-
ca-8f-e0[defaultauthorization]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[category]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[name]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[parentfolder]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[description]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[relativepath]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[parsingname]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[infotip]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[localizedname]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[icon]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[security]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[streamresource]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[streamresourcetype]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[localredirectonly]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[roamable]
   Queries value:
```

```
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[precreate]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[stream]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[publishexpandedpath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[attributes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[foldertypeid]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[initfolderhandler]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local appdata]
  Queries value:              HKLM\software\microsoft\windows media player nss\3.0\servers[0aef9a97-
98cd-4f89-b183-3db737149306]
  Queries value:              HKLM\software\microsoft\windows media player nss\3.0\servers\0aef9a97-
98cd-4f89-b183-3db737149306[defaultauthorization]
  Queries 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]
  Queries value:              HKLM\software\microsoft\windows media player nss\3.0\events\{9360da4b-
0822-41f5-a360-7f9b7a2e9449}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}[reason]
  Queries value:              HKLM\software\microsoft\windows media player nss\3.0\events\{9360da4b-
0822-41f5-a360-7f9b7a2e9449}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}[id]
  Queries value:              HKLM\software\microsoft\windows media player nss\3.0\events\{9360da4b-
0822-41f5-a360-7f9b7a2e9449}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}[data]
  Queries value:              HKLM\software\microsoft\windows media player nss\3.0\events\{9360da4b-
0822-41f5-a360-7f9b7a2e9449}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}[scope]
  Queries value:              HKLM\software\microsoft\windows media player nss\3.0\devices\00-00-00-
00-00-00[alive]
  Queries value:              HKLM\software\microsoft\windows media player nss\3.0\devices\08-00-27-
ca-8f-e0[alive]
  Queries value:              HKLM\software\microsoft\com3[com+enabled]
  Queries value:              HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}\progid[]
  Queries value:              HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}[]
  Queries value:              HKCR\clsid\{e2085f28-feb7-404a-b8e7-
e659bdeaaa02}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}\inprocserver32[]
  Queries value:              HKCR\clsid\{e2085f28-feb7-404a-b8e7-
e659bdeaaa02}\inprocserver32[threadingmodel]
  Queries value:              HKLM\software\microsoft\ole[maxsxshashcount]
  Queries value:              HKCR\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32[]
  Queries value:              HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Queries value:              HKLM\software\microsoft\sqmclient\windows\disabledprocesses[5512633]
  Queries value:              HKLM\software\microsoft\com3[gipactivitybypass]
  Queries value:              HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}\proxystubclsid32[]
  Queries value:              HKCR\clsid\{00020424-0000-0000-c000-000000000046}[]
  Queries value:              HKCR\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32[]
  Queries value:              HKCR\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
  Queries value:              HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}\typelib[]
  Queries value:              HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}\typelib[version]
  Queries value:              HKCR\typelib\{db3442a7-a2e9-4a59-9cb5-f5c1a5d901e5}\1.0\0\win32[]
  Queries value:              HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32[]
  Queries value:              HKLM\software\microsoft\rpc[udtalignmentpolicy]
  Queries value:              HKCR\interface\{00020400-0000-0000-c000-000000000046}\proxystubclsid32[]
  Queries value:              HKCR\clsid\{00020420-0000-0000-c000-000000000046}[]
  Queries value:              HKCR\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32[]
  Queries value:              HKCR\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
  Queries value:              HKCR\interface\{e3bf6178-694e-459f-a5a6-191ea0ffa1c7}\proxystubclsid32[]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\modules\179b8a65-b0f6-41d9-acea-
12006ef9b32a[manifestfile]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\modules\179b8a65-b0f6-41d9-acea-
12006ef9b32a[pluginfile]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\modules\c42d83ff-5958-4af4-a0dd-
ba02fed39662[manifestfile]
  Queries 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]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/bios/4.0[moduleid]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/bios/4.0[isservice]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/flags/1.0[moduleid]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/hwid/4.0[moduleid]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/phone/1.0[moduleid]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2005[moduleid]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/vmd/1.0[moduleid]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/volume/1.0[moduleid]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/eul/1.0[moduleid]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pkc/1.0[moduleid]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/rac/1.0[moduleid]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/spc/1.0[moduleid]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/sequence/1.0[moduleid]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/taskscheduler/1.0[moduleid]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/1.0[moduleid]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/licenserenewal/1.0[moduleid]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/windowsfunctionality/agent/7.0[moduleid]
   Queries value:              HKCR\interface\{0405af4f-8b5c-447c-80f2-b75984a31f3c}\proxystubclsid32[]
   Queries value:              HKCR\interface\{0405af4f-8b5c-447c-80f2-b75984a31f3c}\typelib[]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/windowsfunctionality/agent/7.0[isservice]
   Queries value:              HKCR\interface\{0405af4f-8b5c-447c-80f2-b75984a31f3c}\typelib[version]
   Sets/Creates value:         HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-
409d6c4515e9}\inprocserver32[threadingmodel]
   Sets/Creates value:         HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-
409d6c4515e9}\inprocserver32[]
   Sets/Creates value:         HKLM\software\microsoft\windows media player nss\3.0\events\{6cc10660-
1516-4ed8-94f7-9cadbee645b1}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}[reason]
   Sets/Creates value:         HKLM\software\microsoft\windows media player nss\3.0\events\{6cc10660-
1516-4ed8-94f7-9cadbee645b1}\{b6f6840f-0ce4-4389-be1b-e9c93f9f433b}[id]
   Sets/Creates value:         HKLM\software\microsoft\windows media player nss\3.0\events\{6cc10660-
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]
   Value changes:              HKCU\software\classes\local settings\muicache\27\52c64b7e[languagelist]
   Value changes:              HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32[]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
   Value changes:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[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:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-
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]
```