Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

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

Task ID:	826
Risk Level:	10
Date Processed:	2016-05-18 10:42:32 (UTC)
Processing Time:	62.56 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\26ec828da6d2651f90c74cb275b800cc.exe"
Sample ID:	3329
Type:	basic
Owner:	admin
Label:	26ec828da6d2651f90c74cb275b800cc
Date Added:	2016-05-18 10:30:51 (UTC)
File Type:	PE32:win32:gui
File Size:	184320 bytes
MD5:	26ec828da6d2651f90c74cb275b800cc
SHA256:	2fd94a7ba79df111cbd03365c4ae7ccc17e7dfaba10a30ed3049db2f369c2d4b
Description:	None

Pattern Matching Results

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

Process/Thread Events

Creates process:	C:\windows\temp\26ec828da6d2651f90c74cb275b800cc.exe ["C:\windows\temp\26ec828da6d2651f90c74cb275b800cc.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:2904 C:\Windows\Temp\26ec828da6d2651f90c74cb275b800cc.exe
Reads from process:	PID:2076 C:\Windows\SysWOW64\calc.exe
Writes to process:	PID:2904 C:\Windows\Temp\26ec828da6d2651f90c74cb275b800cc.exe
Writes to process:	PID:340 C:\Windows\explorer.exe
Writes to process:	PID:436 C:\Windows\System32\services.exe
Writes to process:	PID:2132 C:\Windows\System32\sppsvc.exe
Terminates process:	C:\Windows\Temp\26ec828da6d2651f90c74cb275b800cc.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\TermSrvReadyEvent
Creates event:	\BaseNamedObjects\{9E1C6465-1D54-4446-9F99-8639AF243513}
Creates event:	\KernelObjects\MaximumCommitCondition
Creates event:	\Sessions\1\BaseNamedObjects\PRS_EXTERNAL_CHECK_CHANGED_NOTIFY
Creates event:	\Sessions\1\BaseNamedObjects\{43a2b8d7-6fed-4c18-bd36-b4630d61afb5}

File System Events

Creates:	C:\$Recycle.Bin\
Creates:	C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001
Creates:	C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001\$aaa1415b79b8dbbd8bd16c842c1858a2
Creates:	C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001\$aaa1415b79b8dbbd8bd16c842c1858a2\L
Creates:	C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001\$aaa1415b79b8dbbd8bd16c842c1858a2\U
Creates:	C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001\$aaa1415b79b8dbbd8bd16c842c1858a2\@

Creates: C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001\$aaa1415b79b8dbbd8bd16c842c1858a2\n
Creates: C:\Program Files\Windows Defender\en-US:!
Creates: C:\Program Files\Windows Defender\MpAsDesc.dll:!
Creates: C:\Program Files\Windows Defender\MpClient.dll:!
Creates: C:\Program Files\Windows Defender\MpCmdRun.exe:!
Creates: C:\Program Files\Windows Defender\MpCommu.dll:!
Creates: C:\Program Files\Windows Defender\MpEvMsg.dll:!
Creates: C:\Program Files\Windows Defender\MpOAV.dll:!
Creates: C:\Program Files\Windows Defender\MpRTP.dll:!
Creates: C:\Program Files\Windows Defender\MpSvc.dll:!
Creates: C:\Program Files\Windows Defender\MSASCui.exe:!
Creates: C:\Program Files\Windows Defender\MsMpCom.dll:!
Creates: C:\Program Files\Windows Defender\MsMpLics.dll:!
Creates: C:\Program Files\Windows Defender\MsMpRes.dll:!
Creates: C:\$Recycle.Bin\S-1-5-18
Creates: C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2
Creates: C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\L
Creates: C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\U
Creates: C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\@
Creates: C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\n
Creates: C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001\$I5D1DD46B
Creates: C:GAC_MSIL
Creates: C:GAC
Creates: C:GAC_32
Creates: C:GAC_64
Creates: C:\Windows\assembly\GAC_64\Desktop.ini
Creates: C:\Windows\assembly\GAC_32\Desktop.ini
Creates: C:\Windows\System32\LogFiles\Scm\e22a8667-f75b-4ba9-ba46-067ed4429de8
Creates: C:\Windows\System32\LogFiles\Scm\9435f817-fed2-454e-88cd-7f78fda62c48
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
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\WER\ERC
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\WER\ERC\statecache.lock
Opens: C:\Windows\Prefetch\26EC828DA6D2651F90C74CB275B80-7FC87F1F.pf
Opens: C:\Windows
Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\System32\wow64win.dll
Opens: C:\Windows\System32\wow64cpu.dll
Opens: C:\Windows\system32\wow64log.dll
Opens: C:\Windows\SysWOW64
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\windows\temp\D3D8.DLL
Opens: C:\Windows\SysWOW64\d3d8.dll
Opens: C:\windows\temp\VERSION.dll
Opens: C:\Windows\SysWOW64\version.dll
Opens: C:\windows\temp\d3d8thk.dll
Opens: C:\Windows\SysWOW64\d3d8thk.dll
Opens: C:\windows\temp\dwmapi.dll
Opens: C:\Windows\SysWOW64\dwmapi.dll
Opens: C:\windows\temp\opengl32.dll
Opens: C:\Windows\SysWOW64\opengl32.dll
Opens: C:\windows\temp\GLU32.dll
Opens: C:\Windows\SysWOW64\glu32.dll
Opens: C:\windows\temp\DDRAW.dll
Opens: C:\Windows\SysWOW64\ddraw.dll
Opens: C:\windows\temp\DCIMAN32.dll
Opens: C:\Windows\SysWOW64\dciman32.dll
Opens: C:\Windows\SysWOW64\imm32.dll
Opens: C:\Windows\SysWOW64\en-US\setupapi.dll.mui
Opens: C:\windows\temp\MSCAT32.dll
Opens: C:\Windows\SysWOW64\mscat32.dll
Opens: C:\Windows\Temp\26ec828da6d2651f90c74cb275b800cc.exe
Opens: C:\Windows\SysWOW64\apphelp.dll
Opens: C:\Windows\System32\ntdll.dll
Opens: C:\Windows\SysWOW64\ntdll.dll
Opens: C:\Windows\System32\kernel32.dll
Opens: C:\Windows\SysWOW64\kernel32.dll
Opens: C:\Windows\System32\user32.dll
Opens: C:\Windows\SysWOW64\KernelBase.dll
Opens: C:\Windows\SysWOW64\user32.dll
Opens: C:\Windows\SysWOW64\gdi32.dll
Opens: C:\Windows\SysWOW64\lpk.dll
Opens: C:\Windows\SysWOW64\usp10.dll

Opens: C:\Windows\SysWOW64\msvcrt.dll
Opens: C:\Windows\SysWOW64\advapi32.dll
Opens: C:\Windows\SysWOW64\rpcrt4.dll
Opens: C:\Windows\SysWOW64\sspicli.dll
Opens: C:\Windows\SysWOW64\cryptbase.dll
Opens: C:\Windows\SysWOW64\setupapi.dll
Opens: C:\Windows\SysWOW64\cfgmgr32.dll
Opens: C:\Windows\SysWOW64\oleaut32.dll
Opens: C:\Windows\SysWOW64\ole32.dll
Opens: C:\Windows\SysWOW64\devobj.dll
Opens: C:\Windows\SysWOW64\msctf.dll
Opens: C:\Windows\SysWOW64\wintrust.dll
Opens: C:\Windows\SysWOW64\crypt32.dll
Opens: C:\Windows\SysWOW64\msasn1.dll
Opens: C:\windows\temp\untfs.dll
Opens: C:\Windows\SysWOW64\untfs.dll
Opens: C:\windows\temp\Cabinet.dll
Opens: C:\Windows\SysWOW64\cabinet.dll
Opens: C:\Windows\SysWOW64\ws2_32.dll
Opens: C:\Windows\SysWOW64\nsi.dll
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\SysWOW64\mswsock.dll
Opens: C:\Windows\SysWOW64\WSHTCPIP.DLL
Opens: C:\windows\temp\CRYPTSP.dll
Opens: C:\Windows\SysWOW64\cryptsp.dll
Opens: C:\Windows\SysWOW64\rsaenh.dll
Opens: C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-
1001\$aaa1415b79b8dbbd8bd16c842c1858a2\n
Opens: C:\Program Files\Windows Defender
Opens: C:\Program Files\Windows Defender\en-US
Opens: C:\Windows\MSWSOCK.dll
Opens: C:\Windows\System32\mswsock.dll
Opens: C:\Program Files\Windows Defender\MpAsDesc.dll
Opens: C:\Program Files\Windows Defender\MpClient.dll
Opens: C:\Program Files\Windows Defender\MpCmdRun.exe
Opens: C:\Program Files\Windows Defender\MpCommu.dll
Opens: C:\Program Files\Windows Defender\MpEvMsg.dll
Opens: C:\Program Files\Windows Defender\MpOAV.dll
Opens: C:\Program Files\Windows Defender\MpRTP.dll
Opens: C:\Program Files\Windows Defender\MpSvc.dll
Opens: C:\Program Files\Windows Defender\MSASCui.exe
Opens: C:\Program Files\Windows Defender\MsMpCom.dll
Opens: C:\Program Files\Windows Defender\MsMpLics.dll
Opens: C:\Program Files\Windows Defender\MsMpRes.dll
Opens: C:\Program Files\Microsoft Security Client
Opens: C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\n
Opens: C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001
Opens: C:\Windows\assembly
Opens: C:\Windows\assembly\GAC_32\Desktop.ini
Opens: C:\Windows\assembly\GAC_64\Desktop.ini
Opens: C:\Windows\System32\cryptsp.dll
Opens: C:\Windows\System32\rsaenh.dll
Opens: C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\@
Opens: C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\U
Opens: C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-
1001\$aaa1415b79b8dbbd8bd16c842c1858a2\@
Opens: C:\Windows\Temp
Opens: C:\Windows\System32\rundll32.exe
Opens: C:\Windows\Prefetch\RUNDLL32.EXE-39102DB5.pf
Opens: C:\Windows\System32
Opens: C:\Windows\System32\imm32.dll
Opens: C:\Windows\System32\en-US\rundll32.exe.mui
Opens: C:\Windows\System32\BFE.DLL
Opens: C:\Windows\system32\bfe.dll.manifest
Opens: C:\Windows\system32\bfe.dll.123.Manifest
Opens: C:\Windows\system32\bfe.dll.124.Manifest
Opens: C:\Windows\system32\bfe.dll.2.Manifest
Opens: C:\Windows\System32\authz.dll
Opens: C:\Windows\System32\slc.dll
Opens: C:\Windows\System32\sechost.dll
Opens: C:\Windows\System32\LogFiles\Scm\e22a8667-f75b-4ba9-ba46-067ed4429de8
Opens: C:\Windows\System32\Tasks\Microsoft\Windows\WDI\ResolutionHost
Opens: C:\Windows\SysWOW64\calc.exe
Opens: C:\
Opens: C:\Users\Admin\Desktop
Opens: C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp
Opens: C:\Windows\ServiceProfiles
Opens: C:\Windows\System32\sppsvc.exe
Opens: C:\Windows\AppPatch\AppPatch64\sysmain.sdb
Opens: C:\Windows\Prefetch\SPPSVC.EXE-B0F8131B.pf
Opens: C:\Windows\System32\en-US\sppsvc.exe.mui
Opens: C:\Windows\System32\rpcss.dll
Opens: C:\Windows\System32\cryptbase.dll

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

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

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

Windows Registry Events

Creates key:	HKLM\software\wow6432node\microsoft\direct3d\mostrecentapplication
Creates key:	HKCU\software\classes\clsid
Creates key:	HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}
Creates key:	HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\inprocserver32

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

nt\currentversion\gre_initialize
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime compatibility
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\wow6432node\microsoft\direct3d
Opens key: HKLM\software\policies\microsoft\sqmclient\windows
Opens key: HKLM\software\microsoft\sqmclient\windows
Opens key: HKLM\software\wow6432node\microsoft\ole
Opens key: HKLM\software\wow6432node\microsoft\ole\tracing
Opens key: HKLM\software\microsoft\ole\tracing
Opens key: HKLM\software\wow6432node\microsoft\oleaut
Opens key: HKLM\system\currentcontrolset\control\cmf\config
Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\setup
Opens key: HKLM\software\microsoft\windows\currentversion\setup
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\system\currentcontrolset\services\crypt32
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\msasn1
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\26ec828da6d2651f90c74cb275b800cc.exe
Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\appcompat
Opens key: HKLM\software\policies\microsoft\windows\appcompat
Opens key: HKCU\software\microsoft\windows nt\currentversion
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\appcompatflags\custom\26ec828da6d2651f90c74cb275b800cc.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wow64win.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wow64cpu.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wow64.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernelbase.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\usp10.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\lpk.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\gdi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\cryptbase.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\sspicli.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rpcrt4.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\sechost.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\advapi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\user32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msctf.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\imm32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\version.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\d3d8thk.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dwmapi.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\d3d8.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\glu32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dciman32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\cfgmgr32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ole32.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\oleaut32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\devobj.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\setupapi.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ddraw.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\opengl32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msasn1.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\crypt32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wintrust.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mscat32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\cabinet.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\nsi.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ws2_32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\136a17c6
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
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\namespace_catalog5
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
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\software\microsoft\windows nt\currentversion\image file execution options\mswsock.dll
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\wshtcpip.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cryptsp.dll
Opens key:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft base cryptographic
provider v1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rsaenh.dll
Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
Opens key: HKLM\software\policies\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography
Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload
Opens key:
HKLM\software\wow6432node\microsoft\cryptography\deshashsessionkeybackward
Opens key: HKLM\system\currentcontrolset\services\windefend
Opens key: HKLM\system\currentcontrolset\services\windefend\parameters
Opens key: HKLM\system\currentcontrolset\services\windefend\security
Opens key: HKLM\system\currentcontrolset\services\windefend\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\windefend\triggerinfo\0
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\shellserviceobjects\{fd6905ce-
952f-41f1-9a6f-135d9c6622cc}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\shellserviceobjects\{f56f6fdd-
aa9d-4618-a949-c1b91af43b1a}
Opens key: HKLM\software\microsoft\windows\currentversion\run
Opens key: HKLM\software\wow6432node\microsoft\rpc
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\system\setup
Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
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\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0
Opens key: HKLM\software\microsoft\cryptography\offload
Opens key: HKLM\software\microsoft\cryptography\deshashsessionkeybackward
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: HKLM\software\microsoft\windows\currentversion\sidebyside
Opens key: HKU\.default\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKU\.default\software\policies\microsoft\control panel\desktop
Opens key: HKU\.default\control panel\desktop\languageconfiguration
Opens key: HKU\.default\control panel\desktop
Opens key: HKU\.default\control panel\desktop\muicached
Opens key: HKLM\system\currentcontrolset\control\error message instrument\
Opens key: HKLM\system\currentcontrolset\control\error message instrument
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility
Opens key: HKLM\software\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\microsoft\rpc
Opens key: HKLM\system\currentcontrolset\services\bfe
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\system\currentcontrolset\services\aelookupsvc
Opens key: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\alg
Opens key: HKLM\system\currentcontrolset\services\alg\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\appidsvc
Opens key: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\appinfo
Opens key: HKLM\system\currentcontrolset\services\appinfo\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\appmgmt
Opens key: HKLM\system\currentcontrolset\services\appmgmt\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\audioendpointbuilder
Opens key: HKLM\system\currentcontrolset\services\audioendpointbuilder\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\audiosrv
Opens key: HKLM\system\currentcontrolset\services\audiosrv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\axinstsv
Opens key: HKLM\system\currentcontrolset\services\axinstsv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\bdesvc
Opens key: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\bfe\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\bits
Opens key: HKLM\system\currentcontrolset\services\bits\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\browser
Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\bthserv
Opens key: HKLM\system\currentcontrolset\services\bthserv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\certpropsvc
Opens key: HKLM\system\currentcontrolset\services\certpropsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32
Opens key: HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64
Opens key: HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64\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\perfhost
Opens key: HKLM\system\currentcontrolset\services\perfhost\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\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\advanced
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\wow6432node\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
Opens key: HKCR\wow6432node\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
Opens key: HKCU\software\classes\wow6432node\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\progid
Opens key: HKCR\wow6432node\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\wow6432node\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}
Opens key: HKCR\wow6432node\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}
Opens key: HKCU\software\classes\wow6432node\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\progid
Opens key: HKCR\wow6432node\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\wow6432node\clsid\{90aa3a4e-1cba-4233-b8bb-

535773d48449}
Opens key: HKCR\wow6432node\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}
Opens key: HKCU\software\classes\wow6432node\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\progid
Opens key: HKCR\wow6432node\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\progid
Opens key: HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprocserver32
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\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
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\sppsvc.exe
Opens key: HKLM\system\currentcontrolset\control\mui\settings
Opens key: HKLM\software\microsoft\ole
Opens key: HKCU\software\classes\
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\image file execution options\wmpnetwk.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\wmpnetwk.exe
Opens key: HKLM\software\microsoft\oleaut
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\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: 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\software\microsoft\windows nt\currentversion\msasn1
Opens key: HKLM\software\wow6432node\microsoft\drm
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform
Opens key: HKLM\software\microsoft\cryptography\oid
Opens key: HKLM\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-e8-14-9e
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\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: HKLM\software\microsoft\windows\currentversion\action center\providers\com\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
Opens key: HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
Opens key: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
Opens key: HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\treatas
Opens key: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\treatas
Opens key: HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\progid
Opens key: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
Opens key: HKCR\wow6432node\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
Opens key: HKCU\software\classes\wow6432node\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\progid
Opens key: HKCR\wow6432node\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\progid
Opens key: HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprocserver32
Opens key: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprocserver32
Opens key: HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprochandler32
Opens key: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprochandler32
Opens key: HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprochandler
Opens key: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprochandler
Opens key: HKLM\software\microsoft\security center
Opens key: HKLM\software\policies\microsoft\internet explorer\security
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\0
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\1
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\2
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\4
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\0
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\1
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\2
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\4
Opens key: HKCU\software\policies\microsoft\internet explorer
Opens key: HKCU\software\microsoft\internet explorer\security
Opens key: HKLM\software\microsoft\internet explorer\security
Opens key: HKCR\interface\{00000134-0000-0000-c000-000000000046}
Opens key: HKCR\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\zones
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\com\{ca236752-2e77-4386-b63b-0e34774a413d}

Opens key: HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}
Opens key: HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}
Opens key: HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\treatas
Opens key: HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\treatas
Opens key: HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\progid
Opens key: HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}
Opens key: HKCR\wow6432node\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}
Opens key: HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprocserver32
Opens key: HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprocserver32
Opens key: HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprochandler32
Opens key: HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprochandler32
Opens key: HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprochandler
Opens key: HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprochandler
Opens key: HKLM\software\microsoft\wbem\cimom
Opens key: HKLM\software\policies\microsoft\windows\windows error reporting
Opens key: HKLM\software\microsoft\windows\windows error reporting
Opens key: HKCU\software\policies\microsoft\windows\windows error reporting
Opens key: HKCU\software\microsoft\windows\windows error reporting
Opens key: HKCU\software\microsoft\windows\windows error reporting\erc
Opens key: HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}
Opens key: HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}
Opens key: HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\treatas
Opens key: HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\treatas
Opens key: HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\progid
Opens key: HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\progid
Opens key: HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprocserver32
Opens key: HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprocserver32
Opens key: HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprochandler32
Opens key: HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprochandler32
Opens key: HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprochandler
Opens key: HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprochandler
Opens key: HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}
Opens key: HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}\proxystubclsid32
Opens key: HKLM\software\microsoft\msxml60
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001
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\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}
Opens key: HKCR\wow6432node\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\wow6432node\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: HKLM\software\microsoft\windows\currentversion\action center\providers\com\{c8e6f269-b90a-4053-a3be-499afcec98c4}
Opens key: HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}
Opens key: HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}
Opens key: HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\treatas
Opens key: HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\treatas
Opens key: HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\progid
Opens key: HKCR\typelib\{db3442a7-a2e9-4a59-9cb5-f5c1a5d901e5}\1.0\0
Opens key: HKCR\typelib\{db3442a7-a2e9-4a59-9cb5-f5c1a5d901e5}\1.0\0\win64
Opens key: HKCR\typelib\{db3442a7-a2e9-4a59-9cb5-f5c1a5d901e5}\1.0\0\win32
Opens key: HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}
Opens key: HKCR\wow6432node\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}
Opens key: HKCU\software\classes\wow6432node\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\progid
Opens key: HKCR\wow6432node\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\progid
Opens key: HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprocserver32

Opens key: HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprocserver32
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\win64
Opens key: HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprochandler32
Opens key: HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprochandler32
Opens key: HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprochandler
Opens key: HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprochandler
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\software\microsoft\windows\currentversion\policies\system
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: HKLM\software\microsoft\windows\currentversion\action center\providers\com\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
Opens key: HKCU\software\classes\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
Opens key: HKCR\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
Opens key: HKCU\software\classes\wow6432node\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
Opens key: HKCR\wow6432node\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
Opens key: HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}
Opens key: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}
Opens key: HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\treatas
Opens key: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\treatas
Opens key: HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\progid
Opens key: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}
Opens key: HKCR\wow6432node\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}
Opens key: HKCU\software\classes\wow6432node\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\progid
Opens key: HKCR\wow6432node\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\progid
Opens key: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}
Opens key: HKCR\wow6432node\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: HKLM\software\microsoft\windows\currentversion\action center\providers\eventlog\{01979c6a-42fa-414c-b8aa-eee2c8202018}
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: HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprocserver32
Opens key: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprocserver32
Opens key: HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprochandler32
Opens key: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprochandler32
Opens key: HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprochandler
Opens key: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprochandler
Opens key: HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}
Opens key: HKCR\interface\{e3bf6178-694e-459f-a5a6-191ea0ffa1c7}\forward
Opens key: HKCR\wow6432node\interface\{e3bf6178-694e-459f-a5a6-191ea0ffa1c7}\forward
Opens key: HKCR\interface\{e3bf6178-694e-459f-a5a6-191ea0ffa1c7}\typelib
Opens key: HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}
Opens key: HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32
Opens key: HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32
Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\treatas
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\treatas
Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\progid
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\eventlog\{945a8954-c147-4acd-923f-40c45405a658}
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
Opens key: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
Opens key: HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\progid

Opens key: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\progid
Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32
Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler32
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler32
Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\eventlog\{dab69a6a-4d2a-4d44-94bf-e0091898c881}
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\eventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options[disableusermodecallbackfilter]
Queries value: HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch]
Queries value: HKLM\system\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: HKLM\system\currentcontrolset\control\nls\customlocale[empty]
Queries value: HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[alternatecodepage]
Queries value: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value: HKLM\software\wow6432node\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\wow6432node\microsoft\windows nt\currentversion\compatibility32[26ec828da6d2651f90c74cb275b800cc]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\software\wow6432node\microsoft\direct3d[disablemmx]
Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr[disable]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options[disablelocaloverride]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[usefilter]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[untfs.dll]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
Queries value: 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\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\winsock\parameters[transports]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
Queries value:
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\wow6432node\microsoft\cryptography\defaults\provider\microsoft base cryptographic
provider v1.0[type]
Queries value:
HKLM\software\wow6432node\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: 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\protocol_catalog9\catalog_entries64\000000000010[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006[packedcatalogitem]

Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000003[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[current_namespace_catalog]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[providerid]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0[type]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0[image path]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[public]
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:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKU\.default\control panel\desktop[preferreduilanguages]
Queries value: HKU\.default\control
panel\desktop\muicached[machinepreferreduilanguages]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[rundll32]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\system\currentcontrolset\services\bfe[imagepath]
Queries value: HKLM\system\currentcontrolset\services\bfe[type]
Queries value: HKLM\system\currentcontrolset\services\bfe[start]
Queries value: HKLM\system\currentcontrolset\services\bfe[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\bfe[tag]
Queries value: HKLM\system\currentcontrolset\services\bfe[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\bfe[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\bfe[group]
Queries value: HKLM\system\currentcontrolset\services\bfe[objectname]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[datatype0]
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:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[typeahead]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\advanced[typeahead]
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: 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[wow64]
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[wow64]
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[wow64]
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[wow64]
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\services\wmpnetworksvc[objectname]

Queries value: HKLM\system\currentcontrolset\services\wmpnetworksvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wmpnetworksvc[wow64]
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[devicepath]
Queries value: HKLM\software\microsoft\windows media player nss\3.0[upnppingintervaloverrideinseconds]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[objectname]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[wow64]
Queries value: HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
Queries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[requiredprivileges]
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\software\microsoft\windows media foundation\platform[freewpptrace]
Queries value: HKLM\software\wow6432node\microsoft\drm[lastsessionid]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[00000000-0dc9-401d-b9b8-05e4eca4977e]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[0a592d4d-6d8e-403d-9a4a-4d5e94dc5dc5]
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\wow6432node\microsoft\drm[datapath]
Queries value: HKLM\software\wow6432node\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-e8-14-9e]
Queries value: HKLM\software\microsoft\windows media player nss\3.0\devices\08-00-27-e8-14-9e[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\devices\00-00-00-00-00-00[alive]
Queries value: HKLM\software\microsoft\windows media player nss\3.0\devices\08-00-27-e8-14-9e[alive]
Queries value: HKLM\software\microsoft\com3[com+enabled]
Queries value: HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}\progid[]
Queries value: HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}[]
Queries value: HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}\inprocserver32[]
Queries value: HKCR\clsid\{e2085f28-feb7-404a-b8e7-e659bdeaaa02}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\ole[maxsxshashcount]
Queries value: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}[]
Queries value: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprocserver32[]
Queries value: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprocserver32[threadingmodel]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[1b0ac240-cbb8-4d55-8539-9230a44081a5]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[5857d6ca-9732-4454-809b-2a87b70881f8]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[9dac2c1e-7c5c-40eb-833b-323e85a1ce84]
Queries value: HKLM\software\policies\microsoft\internet explorer\security[disablesecuritysettingscheck]
Queries value: HKLM\software\policies\microsoft\internet explorer\security[disablefixsecuritysettings]
Queries value: HKCU\software\microsoft\internet explorer\security[disablefixsecuritysettings]
Queries value: HKCR\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32[]
Queries value: HKLM\software\microsoft\internet

explorer\security[disablefixsecuritysettings]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.106[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.101[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.103[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.100[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.102[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.104[checksetting]
Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll]
Queries value: HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}[]
Queries value: HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprocserver32[]
Queries value: HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\wbem\cimom[logging]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[a0ef609d-0a14-424c-9270-3b2691a0a394]
Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[5512633]
Queries value: HKLM\software\microsoft\com3[gipactivitybypass]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[3e19a300-75d9-4027-86ba-948b70416220]
Queries value: HKLM\software\microsoft\windows\windows error reporting[disabled]
Queries value: HKCU\software\microsoft\windows\windows error reporting[disabled]
Queries value: HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\progid[]
Queries value: HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}[]
Queries value: HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprocserver32[]
Queries value: HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001[profileimagepath]
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: HKCU\software\microsoft\windows\currentversion\action center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.100[checksetting]
Queries value: HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32[]
Queries value: HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\windows error reporting[lastqueuepestertime]
Queries value: HKLM\software\microsoft\windows\windows error reporting[queuepesterinterval]
Queries value: HKCU\software\microsoft\windows\windows error reporting[queuepesterinterval]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.101[checksetting]
Queries value: HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}\typelib[]
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\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}[]
Queries value: HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprocserver32[]
Queries value: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win64[]
Queries value: HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\system[enablelua]
Queries value: HKLM\software\microsoft\rpc[udtalignmentpolicy]
Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}\proxystubclsid32[]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{c8e6f269-b90a-4053-a3be-499afcec98c4}.check.0[checksetting]
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\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}[]
Queries value: HKCR\interface\{e3bf6178-694e-459f-a5a6-191ea0ffa1c7}\proxystubclsid32[]
Queries value: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprocserver32[]
Queries value: HKCU\software\microsoft\windows\currentversion\action

center\providers\eventlog\{01979c6a-42fa-414c-b8aa-eee2c8202018}[lastknownstate]
Queries value: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprocserver32[threadingmodel]
Queries value: HKCR\interface\{e3bf6178-694e-459f-a5a6-191ea0ffa1c7}\typelib[]
Queries value: HKCR\interface\{e3bf6178-694e-459f-a5a6-191ea0ffa1c7}\typelib[version]
Queries value: HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32[]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.100[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.101[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog\{945a8954-c147-4acd-923f-40c45405a658}[lastknownstate]
Queries value: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}[]
Queries value: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[]
Queries value: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{945a8954-c147-4acd-923f-40c45405a658}.check.42[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog\{dab69a6a-4d2a-4d44-94bf-e0091898c881}[lastknownstate]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{dab69a6a-4d2a-4d44-94bf-e0091898c881}.check.100[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}[lastknownstate]
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: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.106[checksetting]
Value changes: HKLM\software\wow6432node\microsoft\direct3d\mostrecentapplication[name]
Value changes: HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32[]
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\protocol_catalog9\catalog_entries64\000000000010[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000003[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[librarypath]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[librarypath]
Value changes: HKLM\system\currentcontrolset\services\browser[start]

Value changes: HKLM\system\currentcontrolset\services\policyagent[start]
Value changes: HKLM\software\microsoft\windows media player nss\3.0\devices[alivedevicecount]
Value changes: HKLM\software\microsoft\windows media player nss\3.0\devices[functionaldmrcount]
Value changes: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform[servicesessionid]
Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.100[checksetting]
Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.101[checksetting]
Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.100[checksetting]