Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 1, Task ID: 3

Task ID:	3
Risk Level:	10
Date Processed:	2016-03-28 07:35:09 (UTC)
Processing Time:	63.6 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\spyeye_injector.exe"
Sample ID:	1
Type:	basic
Owner:	admin
Label:	spyeye_injector.exe
Date Added:	2016-03-28 07:35:09 (UTC)
File Type:	PE32:win32:gui
File Size:	103936 bytes
MD5:	b98bb6d7428c3dbffcfcab2414c6daa2
SHA256:	fc7f54ce456c164452d8429a7fd5f52629a69338f8954e287d2664c03c37e029
Description:	None

Pattern Matching Results

7 Writes to memory of system processes
6 Modifies registry autorun entries
3 HTTP connection - response code 200 (success)
10 Suspicious writeprocess: Spyeye [Banking]
5 Abnormal sleep detected
7 Injects thread into Windows process
6 Writes to system32 folder
3 Connects to local host
2 PE: Nonstandard section
3 Writes to a log file [Info]
4 Terminates process under Windows subfolder
4 Reads process memory
5 PE: Contains compressed section
6 Notifies system about Internet connection change
10 Creates malicious mutex: Spyeye [Banking]
5 Packer: UPX
5 Adds autostart object
5 Installs service

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Packer:	UPX

Process/Thread Events

Creates process:	C:\windows\temp\spyeye_injector.exe ["C:\windows\temp\spyeye_injector.exe"]
Creates process:	C:\WinOldFileq\83A494219A6.exe ["C:\WinOldFileq\83A494219A6.exe"]
Creates process:	C:\Windows\system32\rundll32.exe ["C:\Windows\system32\rundll32.exe" "C:\Windows\system32\WININET.dll",DispatchAPICall 1]
Reads from process:	PID:2840 C:\Windows\System32\rundll32.exe
Reads from process:	PID:2996 C:\Windows\System32\calc.exe
Reads from process:	PID:3048 C:\Windows\System32\rundll32.exe
Reads from process:	PID:3100 C:\Windows\System32\rundll32.exe
Reads from process:	PID:3272 C:\Windows\System32\rundll32.exe
Reads from process:	PID:3368 C:\Windows\System32\rundll32.exe
Reads from process:	PID:3544 C:\Windows\System32\rundll32.exe
Reads from process:	PID:3640 C:\Windows\System32\rundll32.exe
Writes to process:	PID:1184 C:\Windows\explorer.exe
Writes to process:	PID:364 C:\Windows\System32\wininit.exe
Writes to process:	PID:412 C:\Windows\System32\winlogon.exe
Writes to process:	PID:472 C:\Windows\System32\lsass.exe
Writes to process:	PID:480 C:\Windows\System32\lsm.exe
Writes to process:	PID:580 C:\Windows\System32\svchost.exe
Writes to process:	PID:648 C:\Windows\System32\svchost.exe
Writes to process:	PID:700 C:\Windows\System32\svchost.exe
Writes to process:	PID:824 C:\Windows\System32\svchost.exe
Writes to process:	PID:864 C:\Windows\System32\svchost.exe
Writes to process:	PID:972 C:\Windows\System32\svchost.exe
Writes to process:	PID:1164 C:\Windows\System32\dwm.exe
Writes to process:	PID:1256 C:\Windows\System32\spoolsv.exe
Writes to process:	PID:1296 C:\Windows\System32\svchost.exe
Writes to process:	PID:1308 C:\Windows\System32\taskhost.exe
Writes to process:	PID:1384 C:\Program Files\Adobe\Reader 9.0\Reader\reader_sl.exe
Writes to process:	PID:1476 C:\Windows\System32\svchost.exe
Writes to process:	PID:1532 C:\Windows\System32\svchost.exe
Writes to process:	PID:1928 C:\Windows\System32\UIODetect.exe

Writes to process:	PID:2012 C:\Windows\System32\svchost.exe
Writes to process:	PID:1408 C:\Windows\System32\mobsync.exe
Writes to process:	PID:1508 C:\Windows\System32\taskhost.exe
Writes to process:	PID:2360 C:\Windows\System32\wbem\unsecapp.exe
Writes to process:	PID:2424 C:\Windows\System32\wbem\WmiPrvSE.exe
Writes to process:	PID:2508 C:\Windows\System32\conhost.exe
Writes to process:	PID:2520 C:\Windows\Temp\spyeye_injector.exe
Writes to process:	PID:2840 C:\Windows\System32\rundll32.exe
Writes to process:	PID:3048 C:\Windows\System32\rundll32.exe
Writes to process:	PID:3100 C:\Windows\System32\rundll32.exe
Writes to process:	PID:3272 C:\Windows\System32\rundll32.exe
Writes to process:	PID:3368 C:\Windows\System32\rundll32.exe
Writes to process:	PID:3544 C:\Windows\System32\rundll32.exe
Writes to process:	PID:3640 C:\Windows\System32\rundll32.exe
Terminates process:	C:\WinOldFileq\83A494219A6.exe
Terminates process:	C:\Windows\Temp\spyeye_injector.exe
Terminates process:	C:\Windows\System32\rundll32.exe
Terminates process:	C:\Windows\System32\mobsync.exe
Creates remote thread:	C:\Windows\System32\wininit.exe
Creates remote thread:	C:\Windows\System32\taskhost.exe
Creates remote thread:	C:\Windows\System32\wbem\WmiPrvSE.exe
Creates remote thread:	C:\Windows\System32\svchost.exe
Creates remote thread:	C:\Windows\System32\lsm.exe
Creates remote thread:	C:\Windows\System32\lsass.exe
Creates remote thread:	C:\Windows\System32\ivm\ivm-service.exe
Creates remote thread:	C:\Windows\System32\tlntsrv.exe
Creates remote thread:	C:\Windows\explorer.exe
Creates remote thread:	C:\Windows\System32\spoolsv.exe
Creates remote thread:	C:\Windows\System32\UIODetect.exe
Creates remote thread:	C:\Program Files\Adobe\Reader 9.0\Reader\reader_sl.exe
Creates remote thread:	C:\Windows\System32\dwm.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\BaseNamedObjects\RPCController
Creates mutex:	\Sessions\1\BaseNamedObjects\zXeRY3a_PtW|00000000
Creates mutex:	\BaseNamedObjects\AyGQmYCUYy9EACCAm33s95GoSIiY7
Creates mutex:	\BaseNamedObjects\zXeRY3a_PtW|00000000
Creates mutex:	\Sessions\1\BaseNamedObjects_!MSFTHISTORY!_
Creates mutex:	\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!temporary internet files!content.ie5!
Creates mutex:	\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!roaming!microsoft!windows!cookies!
Creates mutex:	\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!history!history.ie5!
Creates mutex:	\Sessions\1\BaseNamedObjects\WininetStartupMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\WininetConnectionMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\WininetProxyRegistryMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\RasPbFile
Creates mutex:	\Sessions\1\BaseNamedObjects_!MSFTHISTORY!_LOW!_
Creates mutex:	\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!temporary internet files!low!content.ie5!
Creates mutex:	\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!roaming!microsoft!windows!cookies!low!
Creates mutex:	\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!history!low!history.ie5!
Creates mutex:	\Sessions\1\BaseNamedObjects\IESQMMUTEX_0_208
Creates mutex:	\Sessions\1\BaseNamedObjects\!IETld!Mutex
Creates mutex:	\BaseNamedObjects\{4388aeff-d440-4264-bcc2-7700746d7aa9}:sqlce_se_lck:3
Creates event:	\BaseNamedObjects\SvcctrlStartEvent_A3752DX
Creates event:	\BaseNamedObjects\BFE_Notify_Event_{a8167df2-f56a-457b-b3f6-28b793eeb458}
Creates event:	\Security\LSA_AUTHENTICATION_INITIALIZED
Creates event:	\BaseNamedObjects\BFE_Notify_Event_{f5a2ffd3-acbf-45b4-8294-75a5daf3fc9b}
Creates event:	\Sessions\1\BaseNamedObjects\DINPUTWINMM
Creates event:	\BaseNamedObjects\SC_AutoStartComplete
Creates event:	\BaseNamedObjects\TermSrvReadyEvent
Creates semaphore:	\Sessions\1\BaseNamedObjects\4FBEA4B1

File System Events

Creates:	C:\WinOldFileq
Creates:	C:\WinOldFileq\
Creates:	C:\WinOldFileq\83A494219A6.exe
Creates:	C:\WinOldFileq\9C413B7B23C1D6D
Creates:	C:\Users\Admin
Creates:	C:\Users\Admin\AppData\Local
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
Creates:	C:\Users\Admin\AppData\Roaming
Creates:	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies

Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\History
Creates: C:\Users\Admin\Favorites
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache
Creates: C:\Windows\Prefetch\RUNDLL32.EXE-1304AE86.pf
Creates: C:\Windows\Prefetch\WMIPRVSE.EXE-1628051C.pf
Creates:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@microsoft[1].txt
Creates:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@microsoft[2].txt
Creates: C:\Windows\system32\wdi
Creates: C:\Windows\system32\wdi\{86432a0b-3c7d-4ddf-a89c-172faa90485d}
Creates: C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-
172faa90485d}\{c77a97ff-682c-4f36-ae8a-88ab35629b3f}
Creates: C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-
172faa90485d}\{c77a97ff-682c-4f36-ae8a-88ab35629b3f}\snapshot.etl
Creates: C:\Windows\system32\wdi\{86432a0b-3c7d-4ddf-a89c-
172faa90485d}\{c77a97ff-682c-4f36-ae8a-88ab35629b3f}
Creates: C:\Windows\System32\wdi\ShutdownPerformanceDiagnostics_SystemData.bin
Creates: C:\Windows\System32\wdi\BootPerformanceDiagnostics_SystemData.bin
Creates: C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-172faa90485d}\S-1-5-21-
2160590473-689474908-1361669368-1002_UserData.bin
Creates: C:\ProgramData
Opens: C:\Windows\Prefetch\SPYEYE_INJECTOR.EXE-619282B0.pf
Opens: C:\Windows\System32
Opens: C:\Windows\System32\sechost.dll
Opens: C:\Windows\System32\kernel32.dll
Opens: C:\
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\System32\ntdll.dll
Opens: C:\WinOldFileq
Opens: C:\WinOldFileq\
Opens: C:\Windows\Temp\spyeye_injector.exe
Opens: C:\WinOldFileq\83A494219A6.exe
Opens: C:\Windows\AppPatch\sysmain.sdb
Opens: C:\WinOldFileq\ui\SwDRM.dll
Opens: C:\Windows\Prefetch\83A494219A6.EXE-0D3DE1A1.pf
Opens: C:\Windows\System32\imm32.dll
Opens: C:\WinOldFileq\MSIMG32.dll
Opens: C:\Windows\System32\msimg32.dll
Opens: C:\WinOldFileq\9C413B7B23C1D6D
Opens: C:\Windows\MSIMG32.dll
Opens: C:\Windows\System32\user32.dll
Opens: C:\Windows\System32\wininet.dll
Opens: C:\Windows\System32\ws2_32.dll
Opens: C:\Windows\System32\advapi32.dll
Opens: C:\Windows\System32\crypt32.dll
Opens: C:\Windows\System32\tzres.dll
Opens: C:\Windows\System32\en-US\tzres.dll.mui
Opens: C:\Windows\Explorer.EXE.Local\
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
Opens: C:\Users\Admin
Opens: C:\Users\Admin\AppData\Local
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\desktop.ini
Opens: C:\Users\Admin\AppData\Roaming
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini
Opens: C:\Windows\System32\mswsock.dll
Opens: C:\Windows\System32\WSHTCPIP.DLL
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\index.dat
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs
Opens: C:\Windows\dnsapi.DLL
Opens: C:\Windows\System32\dnsapi.dll
Opens: C:\windows\temp\spyeye_injector.exe

Opens: C:\Program Files\Adobe\Reader 9.0\Reader\MSIMG32.dll
Opens: C:\Windows\RASAPI32.dll
Opens: C:\Windows\System32\rasapi32.dll
Opens: C:\Windows\rasman.dll
Opens: C:\Windows\System32\rasman.dll
Opens: C:\Windows\rtutils.dll
Opens: C:\Windows\System32\rtutils.dll
Opens: C:\ProgramData\Microsoft\Network\Connections\Pbk\
Opens: C:\Windows\System32\ras
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk
Opens: C:\Windows\sensapi.dll
Opens: C:\Windows\System32\SensApi.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows
Opens: C:\Users\Admin\AppData\Local\Microsoft
Opens: C:\Users\Admin\AppData
Opens: C:\Users
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\Low
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows
Opens: C:\Users\Admin\AppData\Roaming\Microsoft
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low
Opens: C:\Users\Admin\Favorites
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Virtualized
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE\Low
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache\Low
Opens: C:\Windows\System32\Sens.dll
Opens: C:\Windows\System32\stdole2.tlb
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache\Low
Opens: C:\Users\Admin\AppData\Local\Temp\Low
Opens: C:\Users\Admin\AppData\Local\Temp
Opens: C:\Windows\System32\rundll32.exe
Opens: C:\Windows\Prefetch\RUNDLL32.EXE-1304AE86.pf
Opens: C:
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\History.IE5
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5
Opens: C:\Windows\rasadhlp.dll
Opens: C:\Windows\System32\rasadhlp.dll
Opens: C:\Windows
Opens: C:\Windows\AppPatch
Opens: C:\Windows\Globalization
Opens: C:\Windows\Globalization\Sorting
Opens: C:\Windows\System32\en-US
Opens: C:\Windows\System32\apisetschema.dll
Opens: C:\Windows\System32\KernelBase.dll
Opens: C:\Windows\System32\locale.nls
Opens: C:\Windows\System32\gdi32.dll
Opens: C:\Windows\System32\lpk.dll
Opens: C:\Windows\System32\usp10.dll
Opens: C:\Windows\System32\msvcrt.dll
Opens: C:\Windows\System32\imagehlp.dll
Opens: C:\Windows\System32\apphelp.dll
Opens: C:\Windows\AppPatch\AcLayers.dll
Opens: C:\Windows\System32\sspicli.dll
Opens: C:\Windows\System32\rpcrt4.dll
Opens: C:\Windows\System32\shell32.dll
Opens: C:\Windows\System32\shlwapi.dll
Opens: C:\Windows\System32\ole32.dll
Opens: C:\Windows\System32\oleaut32.dll
Opens: C:\Windows\System32\userenv.dll
Opens: C:\Windows\System32\profapi.dll
Opens: C:\Windows\System32\winspool.drv
Opens: C:\Windows\System32\mpr.dll
Opens: C:\Windows\System32\msctf.dll
Opens: C:\Windows\System32\en-US\rundll32.exe.mui
Opens: C:\Windows\System32\urlmon.dll
Opens: C:\Windows\System32\msasn1.dll
Opens: C:\Windows\System32\iertutil.dll
Opens: C:\Windows\System32\uxtheme.dll
Opens: C:\Windows\System32\dwmapi.dll
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
Opens: C:\Windows\WindowsShell.Manifest
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\index.dat
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\Low\index.dat
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\History.IE5\index.dat

Opens: C:\Windows\System32\nsi.dll
Opens: C:\Windows\System32\IPHLPAPI.DLL
Opens: C:\Windows\System32\winnsi.dll
Opens: C:\Windows\System32\nlaapi.dll
Opens: C:\Windows\System32\NapiNSP.dll
Opens: C:\Windows\System32\cryptbase.dll
Opens: C:\Windows\System32\en-US\wininet.dll.mui
Opens: C:\Windows\System32\rpcss.dll
Opens: C:\Windows\System32\pnrpnsp.dll
Opens: C:\Windows\System32\winrnr.dll
Opens: C:\Windows\System32\wship6.dll
Opens: C:\Windows\System32\drivers\etc\hosts
Opens: C:\Windows\System32\FWPUCLNT.DLL
Opens: C:\Windows\system32\WININET.dll.manifest
Opens: C:\Windows\system32\rundll32.exe.Local\
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\History.IE5\desktop.ini
Opens: C:\Windows\Prefetch\IVM-SERVICE.EXE-9090664A.pf
Opens: C:\Windows\Prefetch\UNSECAPP.EXE-A02905A6.pf
Opens: C:\Windows\Prefetch\WMIPRVSE.EXE-1628051C.pf
Opens: C:\Windows\Prefetch\PARANORMAL.EXE-7FD43081.pf
Opens: C:\Windows\Media\Windows Ding.wav
Opens: C:\Windows\system32\wbem\MSIMG32.dll
Opens: C:\Windows\System32\MMDevAPI.dll
Opens: C:\Windows\System32\propsys.dll
Opens: C:\Windows\System32\adtschema.dll
Opens: C:\Windows\System32\msobjs.dll
Opens: C:\Windows\System32\en-US\adtschema.dll.mui
Opens: C:\Users\Admin\Desktop
Opens: C:\Windows\System32\calc.exe
Opens: C:\Windows\System32\en-US\advapi32.dll.mui
Opens: C:\Windows\System32\w32time.dll
Opens: C:\Windows\System32\en-US\w32time.dll.mui
Opens: C:\Windows\System32\en-US\urlmon.dll.mui
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.microsoft[2].txt
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@microsoft[1].txt
Opens: C:\Windows\Prefetch\CALC.EXE-77FDF17F.pf
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@microsoft[2].txt
Opens: C:\Windows\Prefetch
Opens: C:\dump.pcap
Opens: C:\Windows\system32\wdi\{86432a0b-3c7d-4ddf-a89c-172faa90485d}\{c77a97ff-682c-4f36-ae8a-88ab35629b3f}\snapshot.etl
Opens: C:\Windows\System32\WDI\LogFiles\WdiContextLog.etl.002
Opens: C:\Windows\System32\wdi\LogFiles\WdiContextLog.etl.002
Opens: C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-172faa90485d}\{c77a97ff-682c-4f36-ae8a-88ab35629b3f}\snapshot.etl
Opens: C:\Windows\System32\wdi\LogFiles\ShutdownCKCL.etl
Opens: C:\Windows\System32\wdi\LogFiles\WdiContextLog.etl.003
Opens: C:\Windows\System32\wdi\LogFiles\BootCKCL.etl
Opens: C:\Windows\System32\wdi\ShutdownPerformanceDiagnostics_SystemData.bin
Opens: C:\Windows\System32\diagperf.dll
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-Performance%4Operational.evtx
Opens: C:\Windows\System32\wdi\BootPerformanceDiagnostics_SystemData.bin
Opens: C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-172faa90485d}\S-1-5-21-2160590473-689474908-1361669368-1002_UserData.bin
Opens: C:\Windows\System32\drivers\nnetsecl.sys
Opens: C:\Windows\System32\themeservice.dll
Opens: C:\Windows\System32\en-US\themeservice.dll.mui
Opens: C:\Windows\System32\profsvc.dll
Opens: C:\Windows\System32\en-US\profsvc.dll.mui
Opens: C:\Windows\System32\gpsvc.dll
Opens: C:\Windows\System32\en-US\gpsvc.dll.mui
Opens: C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-172faa90485d}
Opens: C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-172faa90485d}\{c77a97ff-682c-4f36-ae8a-88ab35629b3f}
Opens: C:\Windows\System32\esent.dll
Opens: C:\Windows\System32\catroot2
Opens: C:\Windows\System32\catroot2\{127D0A1D-4EF2-11D1-8608-00C04FC295EE}\catdb
Opens: C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
Opens: C:\Windows\System32\catroot2\{127D0A1D-4EF2-11D1-8608-00C04FC295EE}
Opens: C:\Windows\system32\CatRoot2\{127D0A1D-4EF2-11D1-8608-00C04FC295EE}\catdb\

Opens: C:\Windows\system32\CatRoot2\{127D0A1D-4EF2-11D1-8608-00C04FC295EE}
Opens: C:\Windows\system32\CatRoot2
Opens: C:\Windows\system32
Opens: C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
Opens: C:\Windows\system32\CatRoot2\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\catdb\
Opens: C:\Windows\system32\CatRoot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
Opens: C:\Windows\System32\catroot2\edb.chk
Opens: C:\Windows\System32\catroot2\edb.log
Opens: C:\Windows\system32\CatRoot2\edbtmp.log
Opens: C:\Windows\system32\CatRoot2\res1.log
Opens: C:\Windows\system32\CatRoot2\res2.log
Opens: C:\Windows\System32\catroot
Opens: C:\Windows\System32\catroot\{127D0A1D-4EF2-11D1-8608-00C04FC295EE}
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Common-Drivers-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Guest-Integration-Drivers-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Media-Foundation-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Media-Foundation-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Anytime-Upgrade-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Anytime-Upgrade-Package~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Anytime-Upgrade-Results-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Anytime-Upgrade-Results-Package~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Backup-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Backup-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BLB-Client-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BLB-Client-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Branding-Professional-Client-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Branding-Professional-Client-Package~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Branding-Ultimate-Client-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Branding-Ultimate-Client-Package~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BusinessScanning-Feature-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BusinessScanning-Feature-Package~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-LanguagePack-Package~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-LanguagePack-Package-wrapper~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Refresh-LanguagePack-Package~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Wired-Network-Drivers-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-

00C04FC295EE}\Microsoft-Windows-Client-Wired-Network-Drivers-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ClipsInTheLibrary-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ClipsInTheLibrary-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-CodecPack-Basic-Encoder-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-CodecPack-Basic-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-CodecPack-Basic-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-CodecPack-Basic-Package-wrapper~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Modem-Drivers-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Modem-Drivers-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-DesktopWindowManager-uDWM-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Disk-Diagnosis-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Disk-Diagnosis-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Editions-Client-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-EnterpriseEdition-wrapper~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Foundation-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Gadget-Platform-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Gadget-Platform-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GPUPipeline-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GPUPipeline-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientExtensions-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientExtensions-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Help-CoreClientUAPS-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Help-CoreClientUAPS-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Help-CoreClientUAUE-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Help-CoreClientUAUE-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Help-Customization-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Help-Customization-Package~31bf3856ad364e35~x86~en-

US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-HomeBasicEdition-wrapper~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-HomePremiumEdition-wrapper~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ICM-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ICM-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-IE-Troubleshooters-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-IE-Troubleshooters-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-IE-Troubleshooters-Package-wrapper~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-IE-Troubleshooters-Package-wrapper~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-IIS-WebServer-AddOn-2-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-IIS-WebServer-AddOn-2-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-IIS-WebServer-AddOn-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-IIS-WebServer-AddOn-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-IIS-WebServer-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-IIS-WebServer-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Indexing-Service-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Indexing-Service-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-InternetExplorer-Optional-Package~31bf3856ad364e35~x86~~8.0.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-InternetExplorer-Optional-Package~31bf3856ad364e35~x86~en-US~8.0.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-InternetExplorer-Optional-Package-wrapper~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-InternetExplorer-Optional-Package-wrapper~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package~31bf3856ad364e35~x86~~8.0.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package~31bf3856ad364e35~x86~en-US~8.0.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Killbits-Package~31bf3856ad364e35~x86~~8.0.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Links-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Links-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-LocalPack-AU-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-LocalPack-CA-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-LocalPack-GB-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-LocalPack-US-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-LocalPack-ZA-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-MediaCenter-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-MediaCenter-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Media-Format-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Media-Format-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-MediaPlayback-OC-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-MediaPlayback-OC-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-MediaPlayer-DVDRegistration-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Basic-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Basic-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Sensors-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Sensors-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-MobilePC-Client-SideShow-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-MobilePC-Client-SideShow-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-MSMQ-Client-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-MSMQ-Client-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx3-OC-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx3-OC-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetworkDiagnostics-DirectAccessEntry-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NFS-ClientSKU-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NFS-ClientSKU-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-OfflineFiles-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-OfflineFiles-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-OpticalMediaDisc-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-OpticalMediaDisc-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ParentalControls-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ParentalControls-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-PeerDist-Client-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-PeerDist-Client-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-PeerToPeer-Full-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-PeerToPeer-Full-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Personalization-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-

00C04FC295EE}\Microsoft-Windows-PhotoBasicPackage~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PhotoBasicPackage~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PhotoPremiumPackage~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PhotoPremiumPackage~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printer-Drivers-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printer-Drivers-Package~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-Foundation-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-Foundation-Package~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-LocalPrinting-Home-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-PremiumTools-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-PremiumTools-Package~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-XPSServices-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-XPSServices-Package~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ProfessionalEdition~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ProfessionalEdition-
wrapper~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RasCMAK-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RasCMAK-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RasRip-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RasRip-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RDC-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RDC-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RecDisc-SDP-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RecDisc-SDP-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteAssistance-Package-
Client~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteAssistance-Package-Client~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteFX-RemoteClient-Setup-LanguagePack~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteFX-RemoteClient-Setup-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteFX-VM-Setup-LanguagePack~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteFX-VM-Setup-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SampleContent-Music-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SampleContent-Ringtones-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package~31bf3856ad364e35~x86~en-

US~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SecureStartup-Basic-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SecureStartup-Basic-Package~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SecureStartup-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SecureStartup-Package~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-Professional-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-Ultimate-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ServicingBaseline-Ultimate-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ShareMedia-ControlPanel-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ShareMedia-ControlPanel-Package~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Shell-HomeGroup-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Shell-HomeGroup-Package~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Shell-InboxGames-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Shell-InboxGames-Package~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Shell-MultiplayerInboxGames-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Shell-MultiplayerInboxGames-Package~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Shell-PremiumInboxGames-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Shell-PremiumInboxGames-Package~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Shell-SoundThemes-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Sidebar-Killbits-SDP-
Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SimpleTCP-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SimpleTCP-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SnippingTool-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SnippingTool-Package~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SNMP-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SNMP-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-StarterEdition-wrapper~31bf3856ad364e35~x86~~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-StickyNotes-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-StickyNotes-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-StorageService-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-StorageService-Package~31bf3856ad364e35~x86~en-
US~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SUA-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SUA-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SystemRestore-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SystemRestore-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TabletPC-OC-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TabletPC-OC-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Telnet-Client-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Telnet-Client-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Telnet-Server-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Telnet-Server-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TerminalServices-CommandLineTools-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TerminalServices-CommandLineTools-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TerminalServices-MiscRedirection-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TerminalServices-MiscRedirection-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TerminalServices-Publishing-WMIProvider-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TerminalServices-Publishing-WMIProvider-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TerminalServices-RemoteApplications-Client-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TerminalServices-RemoteApplications-Client-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TerminalServices-UsbRedirector-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TerminalServices-UsbRedirector-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TerminalServices-WMIProvider-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TerminalServices-WMIProvider-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TFTP-Client-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TFTP-Client-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Tuner-Drivers-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-UltimateEdition~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-UltimateEdition-wrapper~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-VirtualPC-Licensing-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-VirtualPC-USB-RPM-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-VirtualPC-USB-RPM-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-VirtualXP-Licensing-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WindowsFoundation-LanguagePack-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WindowsMediaPlayer-Troubleshooters-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WindowsMediaPlayer-Troubleshooters-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WinOcr-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WinOcr-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WMI-SNMP-Provider-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WMI-SNMP-Provider-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WMPNetworkSharingService-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WMPNetworkSharingService-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Xps-Foundation-Client-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Xps-Foundation-Client-Package~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Networking-MPSSVC-Rules-BusinessEdition-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Networking-MPSSVC-Rules-UltimateEdition-Package~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\nt5.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\ntexe.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\ntpe.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\ntph.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\ntprint.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\oem2.CAT
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Package_1_for_KB2534111~31bf3856ad364e35~x86~~6.1.1.0.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Package_1_for_KB976902~31bf3856ad364e35~x86~~6.1.1.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Package_for_KB2534111_SP1~31bf3856ad364e35~x86~~6.1.1.0.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Package_for_KB2534111~31bf3856ad364e35~x86~~6.1.1.0.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Package_for_KB976902_RTM~31bf3856ad364e35~x86~~6.1.1.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Package_for_KB976902~31bf3856ad364e35~x86~~6.1.1.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Package_for_KB976932~31bf3856ad364e35~x86~~6.1.0.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Package_for_KB976933~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Package_for_KB976933~31bf3856ad364e35~x86~de-DE~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Package_for_KB976933~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Package_for_KB976933~31bf3856ad364e35~x86~es-ES~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Package_for_KB976933~31bf3856ad364e35~x86~fr-FR~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Package_for_KB976933~31bf3856ad364e35~x86~ja-JP~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnbr002.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnbr003.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnbr004.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnbr005.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnbr006.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnbr007.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnbr008.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnbr009.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnbr00a.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnca003.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnca00a.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnca00b.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnca00c.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnca00d.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnca00e.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnca00f.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnca00g.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnca00h.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnca00i.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnca00x.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnca00y.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnca00z.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnep002.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnep003.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnep004.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnep005.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnep00a.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnep00b.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnep00c.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnep00d.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnep00e.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnep00f.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnep00g.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnep00l.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnfx002.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnge001.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prngt002.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prngt003.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prngt004.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnhp002.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnhp003.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnhp004.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnhp005.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnin002.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnin003.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnin004.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnkm002.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnkm003.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-

00C04FC295EE}\prnkm004.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnkm005.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnky002.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnky003.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnky004.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnky005.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnky006.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnky007.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnky008.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnky009.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnle002.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnle003.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnle004.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnlx002.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnlx003.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnlx004.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnlx005.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnlx006.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnlx007.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnlx008.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnlx009.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnlx00a.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnlx00b.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnlx00c.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnlx00d.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnlx00e.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnlx00v.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnlx00w.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnlx00x.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnlx00y.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnlx00z.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnms002.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnnr002.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnnr003.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnnr004.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnod002.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnok002.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnrc002.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnrc003.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnrc004.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnrc005.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnrc006.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnrc007.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnrc00a.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnrc00b.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnrc00c.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnsa002.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnsh002.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnso002.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnsv002.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnsv003.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnsv004.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnts002.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnts003.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnxx002.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Server-Help-Package.ClientProfessional~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Server-Help-Package.ClientProfessional~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Server-Help-Package.ClientUltimate~31bf3856ad364e35~x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Server-Help-Package.ClientUltimate~31bf3856ad364e35~x86~en-US~6.1.7601.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Windows7SP1-KB976933~31bf3856ad364e35~x86~~6.1.0.17514.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\windows-legacy-whql.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
Opens: C:\Windows\System32\netevent.dll
Opens: C:\Windows\System32\en-US\netevent.dll.mui
Opens: C:\Windows\System32\qmgr.dll
Opens: C:\Windows\System32\bitsperf.dll
Opens: C:\ProgramData
Opens: C:\ProgramData\Microsoft\Network
Opens: C:\ProgramData\Microsoft\Network\Downloader
Opens: C:\Windows\System32\bitsigd.dll
Opens: C:\Windows\System32\upnp.dll
Opens: C:\Windows\System32\FntCache.dll
Opens: C:\Windows\System32\winhttp.dll
Opens: C:\Windows\System32\webio.dll
Opens: C:\Windows\System32\ssdpapi.dll
Opens: C:\Windows\System32\ktmw32.dll
Opens: C:\Windows\System32\ssdpsrv.dll
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache-System.dat
Opens: C:\Windows\Fonts
Opens: C:\Windows\System32\secur32.dll
Opens: C:\Windows\System32\credssp.dll
Opens: C:\Windows\System32\RpcRtRemote.dll
Opens: C:\ProgramData\Microsoft\Network\Downloader\qmgr0.dat
Opens: C:\ProgramData\Microsoft\Network\Downloader\qmgr1.dat
Opens: C:\Windows\Fonts\modern.fon
Opens: C:\Windows\Fonts\roman.fon
Opens: C:\Windows\Fonts\script.fon
Writes to: C:\WinOldFileq\83A494219A6.exe
Writes to: C:\WinOldFileq\9C413B7B23C1D6D
Writes to: C:\Windows\Prefetch\RUNDLL32.EXE-1304AE86.pf
Writes to: C:\Windows\Prefetch\WMIPRVSE.EXE-1628051C.pf
Writes to: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@microsoft[2].txt
Writes to: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@microsoft[1].txt
Writes to: C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-172faa90485d}\{c77a97ff-682c-4f36-ae8a-88ab35629b3f}\snapshot.etl
Writes to: C:\Windows\System32\wdi\ShutdownPerformanceDiagnostics_SystemData.bin
Writes to: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-Performance%4Operational.evtx
Writes to: C:\Windows\System32\wdi\BootPerformanceDiagnostics_SystemData.bin
Writes to: C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-172faa90485d}\S-1-5-21-2160590473-689474908-1361669368-1002_UserData.bin
Writes to: C:\Windows\System32\catroot2\edb.log

Writes to:	C:\Windows\System32\catroot2\{127D0A1D-4EF2-11D1-8608-00C04FC295EE}\catdb
Writes to:	C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
Reads from:	C:\Windows\System32\ntdll.dll
Reads from:	C:\Windows\Temp\spyeye_injector.exe
Reads from:	C:\WinOldFileq\83A494219A6.exe
Reads from:	C:\WinOldFileq\9C413B7B23C1D6D
Reads from:	C:\Windows\System32\user32.dll
Reads from:	C:\Windows\System32\wininet.dll
Reads from:	C:\Windows\System32\ws2_32.dll
Reads from:	C:\Windows\System32\advapi32.dll
Reads from:	C:\Windows\System32\crypt32.dll
Reads from:	C:\Windows\System32\Sens.dll
Reads from:	C:\Windows\System32\stdole2.tlb
Reads from:	C:\Windows\Prefetch\RUNDLL32.EXE-1304AE86.pf
Reads from:	C:\Windows\System32\drivers\etc\hosts
Reads from:	C:\Windows\Media\Windows Ding.wav
Reads from:	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.microsoft[2].txt
Reads from:	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@microsoft[1].txt
Reads from:	C:\Windows\System32\wdi\LogFiles\WdiContextLog.etl.002
Reads from:	C:\Windows\System32\wdi\LogFiles\ShutdownCKCL.etl
Reads from:	C:\Windows\System32\wdi\LogFiles\WdiContextLog.etl.003
Reads from:	C:\Windows\System32\wdi\LogFiles\BootCKCL.etl
Reads from:	C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-172faa90485d}\{c77a97ff-682c-4f36-ae8a-88ab35629b3f}\snapshot.etl
Reads from:	C:\Windows\System32\wdi\ShutdownPerformanceDiagnostics_SystemData.bin
Reads from:	C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-Performance%4Operational.evtx
Reads from:	C:\Windows\System32\wdi\BootPerformanceDiagnostics_SystemData.bin
Reads from:	C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-172faa90485d}\S-1-5-21-2160590473-689474908-1361669368-1002_UserData.bin
Reads from:	C:\Windows\System32\catroot2\{127D0A1D-4EF2-11D1-8608-00C04FC295EE}\catdb
Reads from:	C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
Reads from:	C:\Windows\System32\catroot2\edb.log
Reads from:	C:\Windows\System32\catroot2\edb.chk
Reads from:	C:\Windows\System32\upnp.dll
Reads from:	C:\ProgramData\Microsoft\Network\Downloader\qmgr1.dat
Deletes:	C:\Windows\Temp\spyeye_injector.exe
Deletes:	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@microsoft[1].txt
Deletes:	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@microsoft[2].txt

Network Events

DNS query:	alexeyartemov.com
DNS query:	wpad
DNS query:	www.msftncsi.com
DNS query:	www.microsoft.com
DNS query:	teredo.ipv6.microsoft.com
DNS response:	alexeyartemov.com ⇒ 198.105.244.11
DNS response:	alexeyartemov.com ⇒ 104.239.213.7
DNS response:	a1961.g2.akamai.net ⇒ 219.93.34.33
DNS response:	a1961.g2.akamai.net ⇒ 219.93.34.42
DNS response:	e10088.dspb.akamaiedge.net ⇒ 23.46.28.174
DNS response:	e10088.dspb.akamaiedge.net ⇒ 184.86.231.62
DNS response:	e10088.dspb.akamaiedge.net ⇒ 23.7.35.22
DNS response:	e10088.dspb.akamaiedge.net ⇒ 23.72.44.137
DNS response:	e10088.dspb.akamaiedge.net ⇒ 23.221.32.209
DNS response:	e10088.dspb.akamaiedge.net ⇒ 104.108.42.129
Connects to:	88.198.13.147:443
Connects to:	219.93.34.33:80
Connects to:	198.105.244.11:80
Connects to:	0.0.0.0:80
Connects to:	127.0.0.1:80
Connects to:	23.7.35.22:80
Connects to:	23.72.44.137:80
Connects to:	104.239.213.7:80
Connects to:	23.221.32.209:80
Sends data to:	8.8.8.8:53
Sends data to:	0.0.0.0:547
Sends data to:	88.198.13.147:443
Sends data to:	4.2.2.1:53
Sends data to:	0.0.0.0:5355
Sends data to:	224.0.0.252:5355
Sends data to:	a1961.g2.akamai.net:80 (219.93.34.33)
Sends data to:	alexeyartemov.com:80 (198.105.244.11)
Sends data to:	e10088.dspb.akamaiedge.net:80 (23.7.35.22)

Sends data to: e10088.dspb.akamaiedge.net:80 (23.72.44.137)
Sends data to: alexeyartemov.com:80 (104.239.213.7)
Sends data to: e10088.dspb.akamaiedge.net:80 (23.221.32.209)
Sends data to: 239.255.255.250:1900
Receives data from: 8.8.8.8:53
Receives data from: 4.2.2.1:53
Receives data from: a1961.g2.akamai.net:80 (219.93.34.33)
Receives data from: alexeyartemov.com:80 (198.105.244.11)
Receives data from: e10088.dspb.akamaiedge.net:80 (23.7.35.22)
Receives data from: e10088.dspb.akamaiedge.net:80 (23.72.44.137)
Receives data from: alexeyartemov.com:80 (104.239.213.7)
Receives data from: e10088.dspb.akamaiedge.net:80 (23.221.32.209)
Receives data from: 127.0.0.1:50720

Windows Registry Events

Creates key: HKCU\software\microsoft\windows\currentversion\run
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\1
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\2
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\3
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\4
Creates key: HKCU\software\microsoft\internet explorer\phishingfilter
Creates key: HKCU\software\microsoft\internet explorer\recovery
Creates key: HKCU\software\microsoft\systemcertificates\my
Creates key: HKCU\software\microsoft windows
Creates key: HKLM\software\microsoft\tracing
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\connections
Creates key: HKLM\software\classes
Creates key: HKCU\software\appdatalow
Creates key: HKCU\software\microsoft\internet explorer\internetregistry
Creates key: HKCU\software\microsoft\internet explorer\lowregistry
Creates key: HKCU\software\microsoft\internet explorer\lowregistry\dontshowmethisdialogagain
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache
Creates key: HKCU\software\microsoft\internet explorer\intelliforms
Creates key: HKCU\software\microsoft\internet explorer\toolbar
Creates key: HKCU\software\microsoft\internet explorer\toolbar\webbrowser
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\menuorder\favorites
Creates key: HKCU\software\microsoft\internet explorer\pagesetup
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\passport\lowdamap
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\lowregistry
Creates key: HKCU\software\microsoft\internet explorer\zoom
Creates key: HKCU\software\microsoft\internet explorer\browseremulation\lowmic
Creates key: HKCU\software\microsoft\internet explorer\ietld\lowmic
Creates key: HKCU\software\microsoft\windows nt\currentversion\network\location awareness
Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters
Creates key: HKLM\software
Creates key: HKLM\software\microsoft
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\{1b7b6586-60aa-4cdd-91a5-554248c31a3a}
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\{1b7b6586-60aa-4cdd-91a5-554248c31a3a}\5e-3c-c9-eb-6a-6f
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\5e-3c-c9-eb-6a-6f
Creates key: HKLM\system\currentcontrolset\control\timezoneinformation
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\p3p\history
Creates key: HKLM\system\currentcontrolset\control\diagnostics\performance
Creates key: HKLM\software\microsoft\windows\currentversion\diagnostics\performance\boot
Creates key: HKLM\software\microsoft\windows\currentversion\diagnostics\performance\systemboot
Creates key: HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot
Creates key: HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown
Creates key: HKLM\system\currentcontrolset\services\bits\performance

Creates key: HKLM\software\microsoft\windows\currentversion\bits
Creates key: HKLM\system\currentcontrolset\services\sharedaccess\epoch
Creates key: HKLM\system\currentcontrolset\services\sharedaccess\epoch2
Creates key: HKLM\system\currentcontrolset\services\vss\diag\bits writer
Deletes value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyserver]
Deletes value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyoverride]
Deletes value: HKCU\software\microsoft\windows\currentversion\internet settings[autoconfigurl]
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\
Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKLM\software\policies\microsoft\mui\settings
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop\languageconfiguration
Opens key: HKCU\control panel\desktop
Opens key: HKCU\control panel\desktop\muicached
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key: HKLM\
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\system\currentcontrolset\control\computername
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\system\setup
Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\83a494219a6.exe
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\83a494219a6.exe
Opens key: HKLM\system\currentcontrolset\services\crypt32
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\ole
Opens key: HKLM\software\microsoft\ole\tracing
Opens key: HKLM\software\microsoft\oleaut
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\microsoft\internet explorer
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\user agent
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\user agent
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\user agent
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\user agent
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\user agent\ua tokens
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\user agent\pre platform
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent\pre platform
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent\pre platform
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\user agent\post platform
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent\post platform
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent\post platform
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_browser_emulation
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
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\132b7067
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\software\policies
Opens key: HKCU\software\policies
Opens key: HKCU\software
Opens key: HKLM\software
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\software\policies\microsoft\internet explorer
Opens key: HKLM\software\policies\microsoft\internet explorer\main
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings
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\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013
Opens key: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016
Opens key: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
Opens key: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
Opens key: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
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\policies\microsoft\sqmclient\windows
Opens key: HKLM\software\microsoft\sqmclient\windows
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\psched\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers
Opens key: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\compatibility assistant
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\certdllopenstoreprov
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov\#16
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov\ldap
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
1\certdllopenstoreprov
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
Opens key: HKCU\software\microsoft\systemcertificates\my\physicalstores
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
2160590473-689474908-1361669368-1002
Opens key: HKCU\software\microsoft\systemcertificates\my
Opens key: HKCU\software\microsoft\systemcertificates\my\
Opens key: HKCU\software\microsoft\systemcertificates\my\certificates
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_allow_long_international_filenames
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_allow_long_international_filenames
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_disallow_null_in_response_headers
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_disallow_null_in_response_headers
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_digest_no_extras_in_uri
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_digest_no_extras_in_uri
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
Opens key: HKCU\software\microsoft\systemcertificates\my\crls
Opens key: HKCU\software\microsoft\systemcertificates\my\ctls
Opens key: HKCU\software\microsoft\systemcertificates\my\keys
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_http_username_password_disable
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_http_username_password_disable
Opens key: HKU\.default\control panel\international
Opens key: HKLM\software\microsoft\tracing\explorer_rasapi32
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist
Opens key: HKLM\software\microsoft\tracing\explorer_rasmancs
Opens key: HKCU\software\classes\autoproxytypes
Opens key: HKCR\autoproxytypes
Opens key: HKCU\software\classes\autoproxytypes\application/x-internet-signup
Opens key: HKCR\autoproxytypes\application/x-internet-signup
Opens key: HKCU\software\classes\autoproxytypes\application/x-ns-proxy-autoconfig
Opens key: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig
Opens key: HKCR\clsid\{d597862O-5b9f-11d1-8dd2-O0aaO04abd5e}
Opens key: HKCR\clsid\{d597862O-5b9f-11d1-8dd2-O0aaO04abd5e}\treatas
Opens key: HKCR\clsid\{d597862O-5b9f-11d1-8dd2-O0aaO04abd5e}\progid
Opens key: HKCR\clsid\{d597862O-5b9f-11d1-8dd2-O0aaO04abd5e}\inprocserver32
Opens key: HKCR\clsid\{d597862O-5b9f-11d1-8dd2-O0aaO04abd5e}\inprochandler32
Opens key: HKCR\clsid\{d597862O-5b9f-11d1-8dd2-O0aaO04abd5e}\inprochandler
Opens key: HKCU\software\classes\
Opens key: HKLM\software\classes
Opens key: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d597862O-5b9f-11d1-8dd2-O0aaO04abd5e}-{OOOOOOOO-OOOO-OOOO-OOOO-OOOOOOOOOOOO}-{OOOOOOOO-OOOO-OOOO-OOOO-OOOOOOOOOOOO}
Opens key: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-O0aaO04abd5e}\typelib
Opens key: HKCR\typelib
Opens key: HKCR\typelib\{d597deed-5b9f-11d1-8dd2-O0aaO04abd5e}
Opens key: HKCR\typelib\{d597deed-5b9f-11d1-8dd2-O0aaO04abd5e}\2.0

Opens key: HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}\2.0\0
Opens key: HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}\2.0\0\win32
Opens key: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}
Opens key: HKCR\typelib\{00020430-0000-0000-c000-000000000046}
Opens key: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0
Opens key: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0
Opens key: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rundll32.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\rundll32.exe
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling
Opens key: HKLM\sam\sam\domains\account\groups\000003ea
Opens key: HKLM\sam\sam\domains\account\aliases\000003ea
Opens key: HKLM\sam\sam\domains\account\users\000003ea
Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient
Opens key: HKLM\system\currentcontrolset\services\dns
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
Opens key: HKLM\software\policies\microsoft\system\dnsclient
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip6
Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{8ff7f47b-d658-4061-baea-1709a0196aed}
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{7b9cb019-1924-49a5-867c-a68f334c8d34}
Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\system\currentcontrolset\control\cmf\config
Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder
Opens key: HKCU\appevents\schemes\
Opens key: HKCU\appevents\schemes\apps\.default\open\.current
Opens key: HKLM\software\microsoft\windows nt\currentversion\networklist\profiles\{1b7b6586-60aa-4cdd-91a5-554248c31a3a}
Opens key: HKCU\appevents\schemes\apps\.default\open\.current\active
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\{1b7b6586-60aa-4cdd-91a5-554248c31a3a}
Opens key: HKLM\software\microsoft\rpc
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\content
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\explorer
Opens key: HKLM\software\policies\microsoft\windows\explorer
Opens key: HKCU\software\policies\microsoft\windows\explorer
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: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}\propertybag
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\cookies
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}\propertybag
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\history
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\feedplat
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\iecompat
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\ietld
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\307bda19-07de87e0
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\307bda19
Opens key: HKLM\system\currentcontrolset\control\sqmservicelist
Opens key: HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
Opens key: HKLM\software\microsoft\sqmclient\windows\disabledsessions\
Opens key: HKU\
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\connections
Opens key: HKCU\appevents\schemes\apps\.default\close\.current
Opens key: HKCU\appevents\schemes\apps\.default\close\.current\active
Opens key: HKLM\system\currentcontrolset\services\netbt\linkage
Opens key: HKLM\system\currentcontrolset\services\w32time\timeproviders\vmictimeprovider\parameters\ipc
Opens key: HKLM\software\policies\microsoft\windows\networkconnectivitystatusindicator
Opens key: HKLM\system\currentcontrolset\services\nlasvc\parameters\internet
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\connections
Opens key: HKLM\system\currentcontrolset\control\cryptography\providers
Opens key: HKLM\system\currentcontrolset\control\cryptography\configuration
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\
Opens key: HKLM\software\policies\microsoft\internet explorer\security
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKCU\appevents\schemes\apps\.default\.default\.current
Opens key: HKCU\appevents\schemes\apps\.default\.default\.current\active
Opens key: HKLM\system\currentcontrolset\control\timezoneinformation
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\w. europe standard time\dynamic dst
Opens key: HKLM\system\currentcontrolset\services\w32time\timeproviders\ntpclient
Opens key: HKLM\software\microsoft\windows nt\currentversion\winlogon
Opens key: HKLM\software\policies\microsoft\windows\system
Opens key: HKLM\system\currentcontrolset\services
Opens key: HKLM\system\currentcontrolset\services\w32time
Opens key: HKLM\system\currentcontrolset\services\w32time\parameters

Opens key: HKLM\system\currentcontrolset\services\eventlog\security
Opens key: HKLM\system\currentcontrolset\control\terminal server\winstations
Opens key: HKLM\software\microsoft\systemcertificates\remote desktop\physicalstores
Opens key: HKLM\software\microsoft\systemcertificates\remote desktop
Opens key: HKLM\software\microsoft\systemcertificates\remote desktop\
Opens key: HKLM\software\microsoft\systemcertificates\remote desktop\certificates
Opens key: HKLM\software\microsoft\systemcertificates\remote
desktop\certificates\d30806d4a0b6f6f6a90d99a889009077e446491f
Opens key: HKLM\software\microsoft\systemcertificates\remote desktop\crls
Opens key: HKLM\software\microsoft\systemcertificates\remote desktop\ctls
Opens key: HKLM\software\policies\microsoft\systemcertificates\remote desktop
Opens key: HKLM\software\microsoft\enterprisecertificates\remote
desktop\physicalstores
Opens key: HKLM\software\microsoft\enterprisecertificates\remote desktop
Opens key: HKLM\software\policies\microsoft\windows nt\terminal services
Opens key: HKLM\system\currentcontrolset\control\terminal
server\winstations\console
Opens key: HKLM\system\currentcontrolset\control\terminal server\winstations\eh-tcp
Opens key: HKLM\system\currentcontrolset\control\terminal server\winstations\rdp-
tcp
Opens key: HKLM\software\microsoft\windows nt\currentversion\drivers32
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54849625-5478-4994-a5ba-
3e3b0328c30d}\channelreferences
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54849625-5478-4994-a5ba-
3e3b0328c30d}\channelreferences\0
Opens key:
HKCU\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
Opens key: HKCU\software\microsoft\windows\currentversion\multimedia\midimap
Opens key: HKU\s-1-5-18
Opens key: HKCU\software\classes\applications\calc.exe
Opens key: HKCR\applications\calc.exe
Opens key: HKLM\system\currentcontrolset\services\eventlog\system
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a68ca8b7-004f-d7b6-a698-
07e2de0f1f5d}\channelreferences
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a68ca8b7-004f-d7b6-a698-
07e2de0f1f5d}\channelreferences\0
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{06edcfeb-0fd0-4e53-acca-
a6f8bbf81bcb}\channelreferences
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{06edcfeb-0fd0-4e53-acca-
a6f8bbf81bcb}\channelreferences\0
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
Opens key: HKCU\software\microsoft\internet explorer\ietld
Opens key: HKLM\software\policies\microsoft\netlogon\parameters
Opens key: HKLM\system\currentcontrolset\services\netlogon\parameters
Opens key: HKLM\software\microsoft\rpc\securityservice
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\p3p\history\microsoft.com
Opens key: HKLM\software\policies\microsoft\windows\reliability analysis\wmi
Opens key: HKLM\software\microsoft\reliability analysis\wmi
Opens key: HKLM\software\microsoft\windows\currentversion\winevt
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-
622caee05b0a}
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-
diagnostics-performance/operational
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-
performance/operational
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-
diagnostics-performance/diagnostic
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-
performance/diagnostic
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-
diagnostics-performance/diagnostic/loopback
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-
performance/diagnostic/loopback
Opens key: HKLM\system\currentcontrolset\services\nnetsecl
Opens key: HKLM\system\currentcontrolset\services\themes
Opens key: HKLM\system\currentcontrolset\services\themes\parameters
Opens key: HKLM\system\currentcontrolset\services\profsvc
Opens key: HKLM\system\currentcontrolset\services\profsvc\parameters

Opens key: HKLM\system\currentcontrolset\services\gpsvc
Opens key: HKLM\system\currentcontrolset\services\gpsvc\parameters
Opens key: HKLM\system\currentcontrolset\control\nls\locale
Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
Opens key: HKLM\system\currentcontrolset\control\nls\language groups
Opens key: HKLM\software\policies\microsoft\windows nt\reliability
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0063715b-eeda-4007-9429-ad526f62696e}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{01090065-b467-4503-9b28-533766761087}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{01578f96-c270-4602-ade0-578d9c29fc0c}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{017247f2-7e96-11dc-8314-0800200c9a66}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{017ba13c-9a55-4f1f-8200-323055aac810}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{01979c6a-42fa-414c-b8aa-eee2c8202018}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{02012a8a-adf5-4fab-92cb-ccb7bb3e689a}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{030f2f57-abd0-4427-bcf1-3a3587d7dc7d}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{04268430-d489-424d-b914-0cff741d6684}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{04d66358-c4a1-419b-8023-23b73902de2c}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{05921578-2261-42c7-a0d3-26ddbce6c50d}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{059c3e04-5535-4929-85e1-93030e78f47b}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{05d7b0f0-2121-4eff-bf6b-ed3f69b894d7}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{06184c97-5201-480e-92af-3a3626c5b140}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{06edcfeb-0fd0-4e53-acca-a6f8bbf81bcb}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{07de7879-1c96-41ce-afbd-c659a0e8e643}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{08466062-aed4-4834-8b04-cddb414504e5}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0888e5ef-9b98-4695-979d-e92ce4247224}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{093da50c-0bb9-4d7d-b95c-3bb9fcda5ee8}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{09608c12-c1da-4104-a6fe-b959cf57560a}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{099614a5-5dd7-4788-8bc9-e29f43db28fc}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{09ec9687-d7ad-40ca-9c5e-78a04a5ae993}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0a88862d-20a3-4c1f-b76f-162c55adbf93}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0bd3506a-9030-4f76-9b88-3e8fe1f7cfb6}
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0c478c5b-0351-41b1-8c58-4a6737da32e3}
Opens key:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0d4fdc09-8c27-494a-bda0-505e4fd8adae}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0d759f0f-cff9-4902-8867-eb9e29d7a98b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0dd4d48e-2bbf-452f-a7ec-ba3dba8407ae}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0f177893-4a9c-4709-b921-f432d67f43d5}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0f67e49f-fe51-4e9f-b490-6f2948cc6027}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{11a377e3-be1e-4ee7-abda-81c6eda62e71}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{11a75546-3234-465e-bec8-2d301cb501ac}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{122ee297-bb47-41ae-b265-1ca8d1886d40}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{127e0dc5-e13b-4935-985e-78fd508b1d80}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{13480a22-d79f-4334-9d32-aa239398ad3c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{134ea407-755d-4a93-b8a6-f290cd155023}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{13b197bd-7cee-4b4e-8dd0-59314ce374ce}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1418ef04-b0b4-4623-bf7e-d74ab47bbdaa}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{155cb334-3d7f-4ff1-b107-df8afc3c0363}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{15a7a4f8-0072-4eab-abad-f98a4d666aed}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{15ca44ff-4d7a-4baa-bba5-0998955e531e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{17d6e590-f5fe-11dc-95ff-0800200c9a66}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{17e92e2a-3d08-413e-baeb-a79a262bf486}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{17f14a23-551d-40cc-a086-e4194d64ed4c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{18f4a5fd-fd3b-40a5-8fc2-e5d261c5d02e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{192ede41-9175-4c86-ac02-9d003c9d43ab}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{199fe037-2b82-40a9-82ac-e1d46c792b99}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{19d2c934-ee9b-49e5-aaeb-9cce721d2c65}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1a396961-5f3c-4c71-8310-44c653c0bf8a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1a772f65-be1e-4fc6-96bb-248e03fa60f5}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1a9443d4-b099-44d6-8eb1-829b9c2fe290}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1b562e86-b7aa-4131-badc-b6f3a001407e}

Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1b8b402d-78dc-46fb-bf71-46e64aedf165}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1be1a88d-8e34-4170-9123-f503375bbcef}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1c95126e-7eea-49a9-a3fe-a378b03ddb4d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1d75856d-36a7-4ecb-a3f5-b13152222d29}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1db28f2e-8f80-4027-8c5a-a11f7f10f62d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1edeee53-0afe-4609-b846-d8c0b2075b1f}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1f678132-5938-4686-9fdc-c8ff68f15c85}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1f84007d-19ce-4b15-9e81-8a3dd8eb9ecb}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{206f6dea-d3c5-4d10-bc72-989f03c8b84b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{21b7c16e-c5af-4a69-a74a-7245481c1b97}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{22b6d684-fa63-4578-87c9-effcbe6643c7}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{22fb2cd6-0e7b-422b-a0c7-2fad1fd0e716}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{239cfb83-cbb7-4bbc-a02e-9bdb496aa7c2}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{271c5228-c3fe-4e47-831f-48c3652ce5ac}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{272a979b-34b5-48ec-94f5-7225a59c85a0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{27a8c1e2-eb19-463e-8424-b399df27a216}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{28aa95bb-d444-4719-a36f-40462168127e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2992e9cf-4f99-48f5-a0b6-b99b11cd387d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{29d13147-1c2e-48ec-9994-e29dfe496eb3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2a274310-42d5-4019-b816-e4b8c7abe95c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2d318b91-e6e7-4c46-bd04-bfe6db412cf9}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2e35aaeb-857f-4beb-a418-2e6c0e54d988}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2ed6006e-4729-4609-b423-3ee7bcd678ef}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2f07e2ee-15db-40f1-90ef-9d7ba282188a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2fd7a9a5-b1a1-4fc7-b95c-c32fed818f30}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2ff3e6b7-cb90-4700-9621-443f389734ed}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{30336ed4-e327-447c-9de0-51b652c86108}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{314b2b0d-81ee-4474-b6e0-

c2aaec0ddbde}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{314de49f-ce63-4779-ba2b-d616f6963a88}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{319122a9-1485-4e48-af35-7db2d93b8ad2}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{31f60101-3703-48ea-8143-451f8de779d2}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3239eb6f-c7fc-4953-aa15-646829a4ca4c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{331c3b3a-2005-44c2-ac5e-77220c37d6b4}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{355c44fe-0c8e-4bf8-be28-8bc7b5a42720}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{35ac6ce8-6104-411d-976c-877f183d2d32}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3663a992-84be-40ea-bba9-90c7ed544222}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{36c23e18-0e66-11d9-bbeb-505054503030}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{37945dc2-899b-44d1-b79c-dd4a9e57ff98}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3aa52b8b-6357-4c18-a92e-b53fb177853b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3c6c422b-019b-4f48-b67b-f79a3fa8b4ed}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3cb2a168-fe19-4a4e-bdad-dcf422f13473}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3cb40aaa-1145-4fb8-b27b-7e30f0454316}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3cc2d4af-da5e-4ed4-bcbe-3cf995940483}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3df0c2c1-5a04-4966-9790-df6ef0ccde9c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3f7b2f99-b863-4045-ad05-f6afb62e7af1}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3f9e07bd-0e26-4241-a5a5-28cafa150a75}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{40ab57c2-1c53-4df9-9324-ff7cf898a02c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{40ae003c-6f3d-4590-ae1c-0e8be526b50f}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4214dcd2-7c33-4f74-9898-719ccceec20f}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{422088e6-cd0c-4f99-bd0b-6985fa290bdf}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{43d1a55c-76d6-4f7e-995c-64c711e5cafe}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{43e63da5-41d1-4fbf-aded-1bbed98fdd1d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{46098845-8a94-442d-9095-366a6bcfefa9}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{49c2c27c-fe2d-40bf-8c4e-c3fb518037e7}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4a933674-fb3d-4e8d-b01d-17ee14e91a3e}
Opens key:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4b7eac67-fc53-448c-a49d-7cc6db524da7}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ba32972-6fc5-488a-8368-5da620d05127}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4cb314df-c11f-47d7-9c04-65fb0051561b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4cec9c95-a65f-4591-b5c4-30100e51d870}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4edbe902-9ed3-4cf0-93e8-b8b5fa920299}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ee76bd8-3cf4-44a0-a0ac-3937643e37a3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ef850d8-bf30-4e64-a917-ee21b9be1f0a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4f768be8-9c69-4bbc-87fc-95291d3f9d0c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4fba1227-f606-4e5f-b9e8-fab9ab5740f3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4fcbf664-a33a-4652-b436-9d558983d955}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{50b3e73c-9370-461d-bb9f-26f32d68887d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{50bd1bfd-936b-4db3-86be-e25b96c25898}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{51480c1a-90aa-416e-98fd-4c11f735349b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5322d61a-9efa-4bc3-a3f9-14be95c144f8}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{538cbbad-4877-4eb2-b26e-7caee8f0f8cb}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54164045-7c50-4905-963f-e5bc1eef0cca}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5444519f-2484-45a2-991e-953e4b54c8e0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{546549be-9d63-46aa-9154-4f6eb9526378}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54732ee5-61ca-4727-9da1-10be5a4f773d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54849625-5478-4994-a5ba-3e3b0328c30d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54d5ac20-e14f-4fda-92da-ebf7556ff176}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54ffd262-99fe-4576-96e7-1adb500370dc}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{57e0b31d-de8c-4181-bcd1-f70e880b49fc}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5857d6ca-9732-4454-809b-2a87b70881f8}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{588c5c5a-ffc5-44a2-9a7f-d5e8dbe6efd7}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{588cd2e4-a5b0-492d-a59b-f6dd3e7681c6}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5a24fcdb-1cf3-477b-b422-ef4909d51223}

Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5b004607-1087-4f16-b10e-979685a8d131}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5b0a651a-8807-45cc-9656-7579815b6af0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5b93cdfa-5f51-45e0-9fde-296983129e6c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5bbca4a8-b209-48dc-a8c7-b23d3e5216fb}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5c8bb950-959e-4309-8908-67961a1205d5}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5c9be3e0-3593-4dcd-8f6d-63840923ffee}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5d674230-ca9f-11da-a94d-0800200c9a66}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5d896912-022d-40aa-a3a8-4fa5515c76d7}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5d9e0020-3761-4f36-90c8-38ce6511bd12}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5ec13d8e-4b3f-422e-a7e7-3121a1d90c7a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5f92bc59-248f-4111-86a9-e393e12c6139}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{606a6a38-70ec-4309-b3a3-82ff86f73329}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{614696c9-85af-4e64-b389-d2c0db4ff87b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{617853d6-728b-4b59-8a78-c3a9a5eade92}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{61f044af-9104-4ca5-81ee-cb6c51bb01ab}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{63b530f8-29c9-4880-a5b4-b8179096e7b8}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{63d1e632-95cc-4443-9312-af927761d52a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{63d2bb1d-e39a-41b8-9a3d-52dd06677588}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{651df93b-5053-4d1e-94c5-f6e6d25908d0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{65d341f3-baaa-4c6e-8b20-23d4f1574004}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{65d99466-7a8e-489c-b8e1-962bc945031e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6600e712-c3b6-44a2-8a48-935c511f28c8}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{66a5c15c-4f8e-4044-bf6e-71d896038977}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{676f167f-f72c-446e-a498-eda43319a5e3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67bd1fef-afb2-458d-bcde-3758beb84dec}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67fe2216-727a-40cb-94b2-c02211edb34a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6863e644-dd5d-43a2-a8b5-7a81b46672e6}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{699e309c-e782-4400-98c8-

e21d162d7b7b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6a1f2b00-6a90-4c38-95a5-5cab3b056778}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6a2dc7c1-930a-4fb5-bb44-80b30aebed6c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6a502821-ab44-40c8-b32f-37315d9d52e0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6ad52b32-d609-4be9-ae07-ce8dae937e39}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6addabf4-8c54-4eab-bf4f-fbef61b62eb0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6b1ffe48-5b1e-4793-9f7f-ae926454499d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6b4db0bc-9a3d-467d-81b9-a84c6f2f3d40}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6b93bf66-a922-4c11-a617-cf60d95c133d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6ba132c4-da49-415b-a7f4-31870dc9fe25}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6bba3851-2c7e-4dea-8f54-31e5afd029e3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6c260f2c-049a-43d8-bf4d-d350a4e6611a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6d8a3a60-40af-445a-98ca-99359e500146}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6e400999-5b82-475f-b800-cef6fe361539}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6eb8db94-fe96-443f-a366-5fe0cee7fb1c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6ece3302-fee1-4ea9-8b88-086d459ed976}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{70eb4f03-c1de-4f73-a051-33d13d5413bd}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{712abb2d-d806-4b42-9682-26da01d8b307}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{719be4ed-e9bc-4dd8-a7cf-c85ce8e4975d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7237fff9-a08a-4804-9c79-4a8704b70b87}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7288c9f8-d63c-4932-a345-89d6b060174d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{728b8c72-0f0f-4071-9bcc-27cb3b6dacbe}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{72d211e1-4c54-4a93-9520-4901681b2271}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{73370bd6-85e5-430b-b60a-fea1285808a7}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{73e9c9de-a148-41f7-b1db-4da051fdc327}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{741fc222-44ed-4ba7-98e3-f405b2d2c4b4}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7426a56b-e2d5-4b30-bdef-b31815c1a74a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{747ef6fd-e535-4d16-b510-42c90f6873a1}
Opens key:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{74b4a4b1-2302-4768-ac5b-9773dd456b08}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{74b655a2-8958-410e-80e2-3457051b8dff}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{74c2135f-cc76-45c3-879a-ef3bb1eeaf86}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-0870-49e5-bdce-9d7028279489}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-0936-4a55-9d26-5f298f3180bf}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-0cc6-49da-8cd9-8903a5222aa0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-77b8-4ba8-9474-4f4a9db2f5c6}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-8670-4eb6-b535-3b9d6bb222fd}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-997f-49cf-b49f-ecc50184b75d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-c8ae-4f93-9ca1-683a53e20cb6}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-d017-4d0f-93ab-0b4f86579164}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75f48521-4131-4ac3-9887-65473224fcb2}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{777ba8fe-2498-4875-933a-3067de883070}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{78168022-eca5-41e8-9e17-e8c7fd77aae1}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7839bb2a-2ea3-4eca-a00f-b558ba678bec}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7a67066e-193f-4d3a-82d3-322fee5259de}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7b563579-53c8-44e7-8236-0f87b9fe6594}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7b6bc78c-898b-4170-bbf8-1a469ea43fc5}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7b7838a3-6562-4269-bb7a-97b0d9593882}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7bb5af18-cb16-4007-b813-9d88e9d6f8ef}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7bfcf102-7378-431c-9284-0b968258991a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7c314e58-8246-47d1-8f7a-4049dc543e0b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7d29d58a-931a-40ac-8743-48c733045548}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7d44233d-3055-4b9c-ba64-0d47ca40a232}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7d5387b0-cbe0-11da-a94d-0800200c9a66}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7d7b0c39-93f6-4100-bd96-4dda859652c5}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7da4fe0e-fd42-4708-9aa5-89b77a224885}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7dd42a49-5329-4832-8dfd-43d979153a88}

Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7eafcf79-06a7-460b-8a55-bd0a0c9248aa}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7f2bd991-ae93-454a-b219-0bc23f02262a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7f912b92-21ad-496e-b97a-88622a72bc42}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7f9d83de-8abb-457f-98e8-4ad161449ecc}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{802ec45a-1e99-4b83-9920-87c98277ba9d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8085cb91-900e-4d15-a7d1-921ddce641d8}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8115579e-2bea-4c9e-9ab1-821cc2c98ab0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{820a42d8-38c4-465d-b64e-d7d56ea1d612}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{835b79e2-e76a-44c4-9885-26ad122d3b4d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8360bd0f-a7dc-4391-91a7-a457c5c381e4}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{83ed54f0-4d48-4e45-b16e-726ffd1fa4af}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{84051b98-f508-4e54-82fa-8865c697c3b1}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8429e243-345b-47c1-8a91-2c94caf0daab}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8443ccb7-feb0-4b8d-8e28-8d4c7cb814e8}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{85fe7609-ff4a-48e9-9d50-12918e43e1da}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{86133982-63d7-4741-928e-ef1349b80219}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{869fb599-80aa-485d-bca7-db18d72b7219}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{86efff39-2bdd-4efd-bd0b-853d71b2a9dc}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{87d476fe-1a0f-4370-b785-60b028019693}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8939299f-2315-4c5c-9b91-abb86aa0627d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{899daace-4868-4295-afcd-9eb8fb497561}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{89a2278b-c662-4aff-a06c-46ad3f220bca}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{89b1e9f0-5aff-44a6-9b44-0a07a7ce5845}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8a93b54b-c75a-49b5-a5be-9060715b1a33}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8c63b5a5-b484-4381-892d-edd424582df7}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8c9dd1ad-e6e5-4b07-b455-684a9d879900}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8ce93926-bdae-4409-9155-2fe4799ef4d3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{914ed502-b70d-4add-b758-

95692854f8a3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{91f42016-0b4e-4a4b-9bbb-825d06cbed35}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{91f5fb12-fdea-4095-85d5-614b495cd9de}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{92ae46d7-6d9c-4727-9ed5-e49af9c24cbf}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9363ccd9-d429-4452-9adb-2501e704b810}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{93c05d69-51a3-485e-877f-1806a8731346}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{945a8954-c147-4acd-923f-40c45405a658}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9485fa1e-23cd-49a1-84e3-11d8bc550cb7}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{952773bf-c2b7-49bc-88f4-920744b82c43}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{95353826-4fbe-41d4-9c42-f521c6e86360}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9580d7dd-0379-4658-9870-d5be7d52d6de}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{959f1fac-7ca8-4ed1-89dc-cdfa7e093cb0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{968f313b-097f-4e09-9cdd-bc62692d138b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{96ac7637-5950-4a30-b8f7-e07e8e5734c1}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{96f4a050-7e31-453c-88be-9634f4e02139}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{973143dd-f3c7-4ef5-b156-544ac38c39b6}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{98583af0-fc93-4e71-96d5-9f8da716c6b8}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{98bf1cd3-583e-4926-95ee-a61bf3f46470}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{98e6cfcb-ee0a-41e0-a57b-622d4e1b30b1}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{99806515-9f51-4c2f-b918-1eae407aa8cb}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9988748e-c2e8-4054-85f6-0c3e1cad2470}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9b307223-4e4d-4bf5-9be8-995cd8e7420b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9b6123dc-9af6-4430-80d7-7d36f054fb9f}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9c205a39-1250-487d-abd7-e831c6290539}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9d55b53d-449b-4824-a637-24f9d69aa02f}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9db0fdb5-3b21-440e-a94b-63738a4be5de}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9e03f75a-bcbe-428a-8f3c-d46f2a444935}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9e3b3947-ca5d-4614-91a2-7b624e0e7244}
Opens key:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9e6ae157-d9f7-47e5-8c6d-b17bb6c82a27}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9e95e4d0-4cb4-4b5d-a936-c972d7d08d90}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9f0c4ea8-ec01-4200-a00d-b9701cbea5d8}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9f650c63-9409-453c-a652-83d7185a2e83}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a0c1853b-5c40-4b15-8766-3cf1c58f985a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a0e3d8ea-c34f-4419-a1db-90435b8b21d0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a319d300-015c-48be-acdb-47746e154751}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a3e1697b-a12c-46b9-84d1-7ffe73c4b678}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a402fe09-da6e-45f2-82af-3cb37170ee0c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a50b09f8-93eb-4396-84c9-dc921259f952}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a615acb9-d5a4-4738-b561-1df301d207f8}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a68ca8b7-004f-d7b6-a698-07e2de0f1f5d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a6ad76e3-867a-4635-91b3-4904ba6374d7}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a6f32731-9a38-4159-a220-3d9b7fc5fe5d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a7364e1a-894f-4b3d-a930-2ed9c8c4c811}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a7975c8f-ac13-49f1-87da-5a984a4ab417}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a8106e5c-293a-4cd0-9397-2e6fac7f9749}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a82fda5d-745f-409c-b0fe-18ae0678a0e0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a8a1f2f6-a13a-45e9-b1fe-3419569e5ef2}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a97524f6-064c-4c4e-b74b-1acc87c3700d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{aabf8b86-7936-4fa2-acb0-63127f879dbf}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{aaf44901-5c64-4014-8b6c-a80813937293}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ab0d8ef9-866d-4d39-b83f-453f3b8f6325}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{abce23e7-de45-4366-8631-84fa6c525952}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ac43300d-5fcc-4800-8e99-1bd3f85f0320}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ad5162d8-daf0-4a25-88a7-01cbeb33902e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ad8aa069-a01b-40a0-ba40-948d1d8dedc5}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ae4bd3be-f36f-45b6-8d21-bdd6fb832853}

Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{aea1b4fa-97d1-45f2-a64c-4d69fffd92c9}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{af0a5a6d-e009-46d4-8867-42f2240f8a72}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{af2e340c-0743-4f5a-b2d3-2f7225d215de}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{af9cc194-e9a8-42bd-b0d1-834e9cfab799}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b03d4051-3564-4e93-93db-3c34f1b5b503}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b059b83f-d946-4b13-87ca-4292839dc2f2}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b1bebb9a-24aa-4b83-9e4a-38c2a9a44377}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b1c94ed9-ac9b-410e-aa48-4ffc5e45f4e3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b1f90b27-4551-49d6-b2bd-dfc6453762a6}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b2a40f1f-a05a-4dfd-886a-4c4f18c4334c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b3eee223-d0a9-40cd-adfc-50f1888138ab}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b44aec44-38f4-4b59-8df3-10306abf19b2}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b5fd844a-01d4-4b10-a57f-58b13b561582}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b65471e1-019d-436f-bc38-e15fa8e87f53}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b675ec37-bdb6-4648-bc92-f3fdc74d3ca2}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b92cf7fd-dc10-4c6b-a72d-1613bf25e597}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b977cf02-76f6-df84-cc1a-6a4b232322b6}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b98f0db6-26e2-4a66-89fc-32a9a6a9af61}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b9da9fe6-ae5f-4f3e-b2fa-8e623c11dc75}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ba093605-3909-4345-990b-26b746adee0a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bbe94f36-f8dc-4c33-8227-81602b7a3d53}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bc2eeeec-b77a-4a52-b6a4-dffb1b1370cb}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bc97b970-d001-482f-8745-b8d7d5759f99}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bd12f3b8-fc40-4a61-a307-b7a013a069c1}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bd2d1dae-d678-4e10-9667-21cba2aa70c3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bd2f4252-5e1e-49fc-9a30-f3978ad89ee2}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bdb462fc-a297-49a2-bf2e-4f1809e12abc}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{be69781c-b63b-41a1-8e24-

a4fc7b3fc498}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{be932b00-0f8e-4386-ab89-873f7d0274aa}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bf406804-6afa-46e7-8a48-6c357e1d6d61}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c02afc2b-e24e-4449-ad76-bcc2c2575ead}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c06ed57a-a7bd-42d7-b5ff-77a9dec5732d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c100becc-d33a-4a4b-bf23-bbef4663d017}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c100becf-d33a-4a4b-bf23-bbef4663d017}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c26c4f3c-3f66-4e99-8f8a-39405cfed220}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c2fa0899-8a10-412b-a42e-9e5b284a2437}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c4636a1e-7986-4646-bf10-7bc3b4a76e8e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c514638f-7723-485b-bcfc-96565d735d4a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c6bf6832-f7bd-4151-ac21-753ce4707453}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c76baa63-ae81-421c-b425-340b4b24157f}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c7bde69a-e1e0-4177-b6ef-283ad1525271}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c882ff1d-7585-4b33-b135-95c577179137}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c88a4ef5-d048-4013-9408-e04b7db2814a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c89b991e-3b48-49b2-80d3-ac000dfc9749}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c8f7689f-3692-4d66-b0c0-9536d21082c9}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c914f0df-835a-4a22-8c70-732c9a80c634}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c91ef675-842f-4fcf-a5c9-6ea93f2e4f8b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c9bdb4eb-9287-4c8e-8378-6896f0d1c5ef}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ca4e628d-8567-4896-ab6b-835b221f373f}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ca5ba219-c0d4-4efa-9ceb-72aff92672b0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cab2b8a5-49b9-4eec-b1b0-fac21da05a3b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cad2d809-03d9-4f46-9cf4-72aa4f04b6b9}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cb070027-1534-4cf3-98ea-b9751f508376}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cb587ad1-cc35-4ef1-ad93-36cc82a2d319}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cbda4dbf-8d5d-4f69-9578-be14aa540d22}
Opens key:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cd032e15-15ad-4da4-afc6-03bf83516195}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cdc05e28-c449-49c6-b9d2-88cf761644df}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cdead503-17f5-4a3e-b7ae-df8cc2902eb9}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ce20d1c3-a247-4c41-bcb8-3c7f52c8b805}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ce8dee0b-d539-4000-b0f8-77bed049c590}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cf3f502e-b40d-4071-996f-00981edf938e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfaa5446-c6c4-4f5c-866f-31c9b55b962d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d02a9c27-79b8-40d6-9b97-cf3f8b7b5d60}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d1bc9aff-2abf-4d71-9146-ecb2a986eb85}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d1d93ef7-e1f2-4f45-9943-03d245fe6c00}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d4263c98-310c-4d97-ba39-b55354f08584}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d53270e3-c8cf-4707-958a-dad20c90073c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d5c25f9a-4d47-493e-9184-40dd397a004d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d6f68875-cdf5-43a5-a3e3-53ffd683311c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d8975f88-7ddb-4ed0-91bf-3adf48c48e0c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dab065a9-620f-45ba-b5d6-d6bb8efedee9}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dab3b18c-3c0f-43e8-80b1-e44bc0dad901}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{db00dfb6-29f9-4a9c-9b3b-1f4f9e7d9770}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dbe9b383-7cf3-4331-91cc-a3cb16a3b538}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dd5ef90a-6398-47a4-ad34-4dcecdef795f}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dd70bc80-ef44-421b-8ac3-cd31da613a4e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dd85457f-4e2d-44a5-a7a7-6253362e34dc}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{de513a55-c345-438b-9a74-e18cac5c5cc5}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{de7b24ea-73c8-4a09-985d-5bdadcfa9017}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dea07764-0790-44de-b9c4-49677b17174f}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ded165cf-485d-4770-a3e7-9c5f0320e80c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{df32a572-0b4b-44be-b09b-72084fdbf879}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e01b1a7c-c5c9-4e67-99a9-5e85acfb2e10}

Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e04fe2e0-c6cf-4273-b59d-5c97c9c374a4}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e0a40b26-30c4-4656-bc9a-74a5c3a0b2ec}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e104fb41-6b04-4f3a-b47d-f0df2f02b954}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e1dd7e52-621d-44e3-a1ad-0370c2b25946}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e23b33b0-c8c9-472c-a5f9-f2bdfea0f156}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e2816346-87f4-4f85-95c3-0c79409aa89d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e4480490-85b6-11dd-ad8b-0800200c9a66}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e46eead8-0c54-4489-9898-8fa79d059e0e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e4d53f84-7de3-11d8-9435-505054503030}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e53c6823-7bb8-44bb-90dc-3f86090d48a6}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e595f735-b42a-494b-afcd-b68666945cd3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e5ba83f6-07d0-46b1-8bc7-7e669a1d31dc}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e6307a09-292c-497e-aad6-498f68e2b619}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e670a5a2-ce74-4ab4-9347-61b815319f4c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e7558269-3fa5-46ed-9f4d-3c6e282dde55}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e7ef96be-969f-414f-97d7-3ddb7b558ccc}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e8316a2d-0d94-4f52-85dd-1e15b66c5891}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e837619c-a2a8-4689-833f-47b48ebd2442}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e856c26a-e105-4683-a948-6920dcc42e45}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e978f84e-582d-4167-977e-32af52706888}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eb3deb18-d1de-4897-8502-a230ad03db8a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ed6b3ba8-95b2-4cf5-a317-d4af7003884c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{edd08927-9cc4-4e65-b970-c2560fb5c289}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ee4f43b5-03eb-41d2-a28c-ba8bee529247}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-82fd4940b820}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ef1cc15b-46c1-414e-bb95-e76b077bd51e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f0db7ef8-b6f3-4005-9937-feb77b9e1b43}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f230d19a-5d93-47d9-a83f-

53829edfb8df}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f2c628ae-d26c-4352-9c45-74754e1e2f9f}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f3c5e28e-63f6-49c7-a204-e48a1bc4b09d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f3f14ff3-7b80-4868-91d0-d77e497b025e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f404b94e-27e0-4384-bfe8-1d8d390b0aa3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f4aed7c7-a898-4627-b053-44a7caa12fcd}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f5344219-87a4-4399-b14a-e59cd118abb8}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f557ace2-bcf8-4994-8e4b-42368a6f078a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f5d05b38-80a6-4653-825d-c414e4ab3c68}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f61cefc0-aa2e-11da-a746-0800200c9a66}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f6da35ce-d312-41c8-9828-5a2e173c91b6}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f82fb576-e941-4956-a2c7-a0cf83f6450a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f997cd11-0fc9-4ab4-acba-bc742a4c0dd3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{fbcfac3f-8459-419f-8e48-1f0b49cdb85e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{fc3bc8a7-2f61-449c-a8b4-22ac22058f92}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{fc65ddd8-d6ef-4962-83d5-6e5cfe9ce148}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{fc6f77dd-769a-470e-bcf9-1b6555a118be}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{fd771d53-8492-4057-8e35-8c02813af49b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ffdb9886-80f3-4540-aa8b-b85192217ddf}
Opens key: HKLM\system\currentcontrolset\services\eventlog
Opens key: HKLM\system\currentcontrolset\services\eventlog\application\eventlog
Opens key: HKLM\system\currentcontrolset\services\eventlog\hardwareevents\eventlog
Opens key: HKLM\system\currentcontrolset\services\eventlog\internet explorer\eventlog
Opens key: HKLM\system\currentcontrolset\services\eventlog\key management service\eventlog
Opens key: HKLM\system\currentcontrolset\services\eventlog\media center\eventlog
Opens key: HKLM\system\currentcontrolset\services\eventlog\security\eventlog
Opens key: HKLM\system\currentcontrolset\services\eventlog\system\eventlog
Opens key: HKLM\system\currentcontrolset\services\bits
Opens key: HKLM\system\currentcontrolset\services\bits\parameters
Opens key: HKLM\software\microsoft\windows\currentversion\bits
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}\propertybag
Opens key: HKLM\system\currentcontrolset\control\backuprestore\filesnottobackup
Opens key: HKLM\software\policies\microsoft\windows\bits
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\com3

Opens key: HKLM\system\currentcontrolset\services\fontcache
Opens key: HKLM\system\currentcontrolset\services\fontcache\parameters
Opens key: HKLM\system\currentcontrolset\services\ssdpsrv
Opens key: HKLM\system\currentcontrolset\services\ssdpsrv\parameters
Opens key: HKLM\software\microsoft\upnp control point
Opens key: HKLM\software\microsoft\windows nt\currentversion\fonts
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft base cryptographic provider v1.0
Opens key: HKLM\software\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography\offload
Opens key: HKLM\software\microsoft\cryptography\deshashsessionkeybackward
Opens key: HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli
Opens key: HKLM\system\currentcontrolset\control\securityproviders
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll
Opens key: HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
Opens key: HKLM\software\microsoft\rpc\extensions
Opens key: HKLM\system\currentcontrolset\services\bfe
Opens key: HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}
Opens key: HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}\proxystubclsid32
Opens key: HKCR\clsid\{00020424-0000-0000-c000-000000000046}
Opens key: HKCR\clsid\{00020424-0000-0000-c000-000000000046}\treatas
Opens key: HKCR\clsid\{00020424-0000-0000-c000-000000000046}\progid
Opens key: HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32
Opens key: HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprochandler32
Opens key: HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprochandler
Opens key: HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}\forward
Opens key: HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}\typelib
Opens key: HKCR\typelib\{db3442a7-a2e9-4a59-9cb5-f5c1a5d901e5}
Opens key: HKCR\typelib\{db3442a7-a2e9-4a59-9cb5-f5c1a5d901e5}\1.0
Opens key: HKCR\typelib\{db3442a7-a2e9-4a59-9cb5-f5c1a5d901e5}\1.0\0
Opens key: HKCR\typelib\{db3442a7-a2e9-4a59-9cb5-f5c1a5d901e5}\1.0\0\win32
Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}
Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\treatas
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\progid
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprochandler32
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprochandler
Opens key: HKLM\software\policies\microsoft\windows\bits\throttling
Opens key: HKLM\system\currentcontrolset\services\vss\vssaccesscontrol
Opens key: HKLM\sam\sam\domains\builtin\groups\00000220
Opens key: HKLM\sam\sam\domains\builtin\aliases\00000220
Opens key: HKLM\sam\sam\domains\builtin\groups\names\administrators
Opens key: HKLM\sam\sam\domains\builtin\aliases\names\administrators
Opens key: HKLM\sam\sam\domains\builtin\groups\names\system
Opens key: HKLM\sam\sam\domains\builtin\aliases\names\system
Opens key: HKLM\sam\sam\domains\builtin\users\names\system
Opens key: HKLM\sam\sam\domains\account\groups\names\system
Opens key: HKLM\sam\sam\domains\account\aliases\names\system
Opens key: HKLM\sam\sam\domains\account\users\names\system
Opens key: HKLM\sam\sam\domains\builtin\groups\00000227
Opens key: HKLM\sam\sam\domains\builtin\aliases\00000227
Opens key: HKLM\sam\sam\domains\builtin\groups\names\backup operators
Opens key: HKLM\sam\sam\domains\builtin\aliases\names\backup operators
Opens key: HKLM\sam\sam\domains\builtin\groups\names\network service
Opens key: HKLM\sam\sam\domains\builtin\aliases\names\network service
Opens key: HKLM\sam\sam\domains\builtin\users\names\network service
Opens key: HKLM\sam\sam\domains\account\groups\names\network service
Opens key: HKLM\sam\sam\domains\account\aliases\names\network service
Opens key: HKLM\sam\sam\domains\account\users\names\network service
Opens key: HKLM\sam\sam\domains\builtin\groups\names\local service
Opens key: HKLM\sam\sam\domains\builtin\aliases\names\local service
Opens key: HKLM\sam\sam\domains\builtin\users\names\local service
Opens key: HKLM\sam\sam\domains\account\groups\names\local service
Opens key: HKLM\sam\sam\domains\account\aliases\names\local service
Opens key: HKLM\sam\sam\domains\account\users\names\local service
Opens key: HKLM\system\currentcontrolset\services\vss\settings
Opens key: HKLM\system\currentcontrolset\services\vss\diag
Opens key: HKLM\system\currentcontrolset\services\vss\diag\bits writer
Opens key: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{faf53cc4-bd73-4e36-83f1-2b23f46e513e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}
Queries value: HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value:

HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup[systemsetupinprogress]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\layers[c:\winoldfileq\83a494219a6.exe]
Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[83a494219a6]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
Queries value: HKLM\software\microsoft\internet explorer[version]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[compatible]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[compatible]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[user
agent]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation[explorer.exe]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation[*]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[0cfe0455-93ba-440d-
a3fe-553973d0b723]
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\control\wmi\security[797fabac-7b58-4796-
b924-d51178a59ce4]
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: HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
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: HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablepassport]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[idnenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[cachemode]
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\software\policies\microsoft\windows\currentversion\internet settings[enablehttp1_1]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[enablehttp1_1]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[enablehttp1_1]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[proxyhttp1.1]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[proxyhttp1.1]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyhttp1.1]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[enablenegotiate]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablebasicoverclearchannel]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol[feature_clientauthcertfilter]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol[feature_clientauthcertfilter]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[clientauthbuiltinui]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[syncmode5]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache[sessionstarttimedefaultdeltasecs]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache[signature]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[peruseritem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[peruseritem]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[cache]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[local appdata]
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: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
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: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
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: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cachelimit]
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\software\microsoft\windows nt\currentversion\compatibility32[lsass]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
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: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[history]
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: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\history[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\history[cachelimit]
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\software\microsoft\sqmclient\windows[ceipenable]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\psched[winsock 2.0 provider id]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip[winsock 2.0 provider id]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
Queries value: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\compatibility assistant[logignoremonitorreason]
Queries value: HKLM\system\currentcontrolset\services\crypt32[diaglevel]
Queries value: HKLM\system\currentcontrolset\services\crypt32[diagmatchanymask]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\domstore[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\domstore[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\domstore[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\domstore[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\domstore[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\extensible cache\feedplat[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[displayscriptdownloadfailureui]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsservername]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsapiforcrack]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
2160590473-689474908-1361669368-1002[profileimagepath]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[utf8servernameres]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[connectretries]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]

Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[receivetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablentlmpreauth]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[scavengecachelowerbound]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[certcachenovalidate]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache[scavengecachefilelifetime]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings\5.0\cache[scavengecachefilelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache[scavengecachefilelimit]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache[scavengecachefilelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[httpdefaultexpirytimesecs]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[ftpdefaultexpirytimesecs]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[explorer.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablecachingofsslpages]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[perusercookies]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[leashlegacycookies]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[dialupuselansettings]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[dialupuselansettings]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[sendextracrlf]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[wpadsearchalldomains]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[bypasshttpnocachecheck]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[bypasshttpnocachecheck]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[bypassssl nocachecheck]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[bypassssl nocachecheck]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[enablehttptrace]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[nocheckautodialoverride]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[nocheckautodialoverride]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[dontusednsloadbalancing]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[dontusednsloadbalancing]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[sharecredswithwinhttp]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[mimeexclusionlistforcache]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[headerexclusionlistforcache]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[dnscacheenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[dnscacheentries]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[dnscachetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonpost]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnalwaysonpost]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonzonecrossing]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonbadcertrecving]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonpostredirect]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[alwaysdrainonredirect]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonhttpstohttpredirect]
Queries value: HKLM\software\microsoft\windows\currentversion\internet

settings[tcpautotuning]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad[wpadoverride]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[enableautodial]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[nonetautodial]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[globaluseroffline]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[badproxyexpirestime]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[disablebranchcache]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_http_username_password_disable[explorer.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_http_username_password_disable[*]
Queries value: HKLM\software\microsoft\tracing[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\explorer_rasapi32[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\explorer_rasapi32[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\explorer_rasapi32[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\explorer_rasapi32[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\explorer_rasapi32[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\explorer_rasapi32[filedirectory]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[programdata]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[appdata]
Queries value: HKLM\software\microsoft\tracing\explorer_rasmancs[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\explorer_rasmancs[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\explorer_rasmancs[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\explorer_rasmancs[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\explorer_rasmancs[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\explorer_rasmancs[filedirectory]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[proxysettingsperuser]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[migrateproxy]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyenable]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyserver]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyoverride]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[autoconfigurl]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\connections[savedlegacysettings]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\connections[defaultconnectionsettings]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[autoconfigcustomua]
Queries value: HKCR\autoproxytypes\application/x-internet-signup[dllfile]
Queries value: HKCR\autoproxytypes\application/x-internet-signup[fileextensions]
Queries value: HKCR\autoproxytypes\application/x-internet-signup[default]
Queries value: HKCR\autoproxytypes\application/x-internet-signup[flags]
Queries value: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[dllfile]
Queries value: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[fileextensions]
Queries value: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[default]
Queries value: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[flags]
Queries value: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}[]
Queries value: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprocserver32[]
Queries value: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[favorites]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassname]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[ownersid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[firinginterfaceiid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[customconfigclsid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[description]

Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[typelib]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[multiinterfacepublisherfilterclsid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[allowinprocactivation]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[fireinparallel]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[eventclasspartitionid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassapplicationid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[parallelfiringtimeout]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[allowperuserinprocactivation]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[allowperuseractivateasactivator]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[allowperusermoniker]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[serialfiringtimeout]
Queries value: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}\typelib[]
Queries value: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}\typelib[version]
Queries value: HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}\2.0\0\win32[]
Queries value: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}[interfacehelperdisabletypelib]
Queries value: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}[interfacehelperdisableall]
Queries value: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}[interfacehelperuser]
Queries value: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32[]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling[explorer.exe]
Queries value: HKLM\sam\sam\domains\account\users\000003ea[v]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]

Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6[winsock 2.0 provider id]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache[shutdownonidle]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[searchlist]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[enabledhcp]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpv6domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpnameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[enabledhcp]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[dhcpnameserver]
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[maxnumberofaddressestoregister]

Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[enablemulticast]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[disabledynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[enableadapterdomainnameregistration]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[maxnumberofaddressestoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[enablemulticast]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
Queries value: HKCU\software\microsoft\windows nt\currentversion\appcompatflags[showdebuginfo]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[rundll32]
Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
Queries value: HKCU\appevents\schemes[]
Queries value: HKCU\appevents\schemes\apps\.default\open\.current[]
Queries value: HKCU\appevents\schemes\apps\.default\open\.current[default flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad[wpadlastnetwork]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[autoproxydetecttype]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache[signature]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\content[peruseritem]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-

ba85-6007caedcf9d}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[initfolderhandler]
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:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[category]
Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\content[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\content[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\cookies[peruseritem]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[infotip]

Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[initfolderhandler]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-

a03a-e3ef65729f3d}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\cookies[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\cookies[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\history[peruseritem]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\lowcache\history[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\history[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\feedplat[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\feedplat[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\feedplat[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\feedplat[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\feedplat[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\iecompat[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\iecompat[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\iecompat[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\iecompat[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\iecompat[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\ietld[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\ietld[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\ietld[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\ietld[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\ietld[cacheoptions]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[rundll32.exe]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
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: HKCU\appevents\schemes\apps\.default\close\.current[]
Queries value: HKCU\appevents\schemes\apps\.default\close\.current[default flags]
Queries value: HKLM\system\currentcontrolset\services\netbt\linkage[export]
Queries value:
HKLM\software\policies\microsoft\windows\networkconnectivitystatusindicator[noactiveprobe]
Queries value:
HKLM\system\currentcontrolset\services\nlasvc\parameters\internet[activewebprobehost]
Queries value:
HKLM\system\currentcontrolset\services\nlasvc\parameters\internet[activewebprobepath]
Queries value:
HKLM\system\currentcontrolset\services\nlasvc\parameters\internet[activewebprobecontent]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\connections[winhttpsettings]
Queries value: HKLM\software\microsoft\windows nt\currentversion\networklist\profiles\{1b7b6586-60aa-4cdd-91a5-554248c31a3a}[profilename]
Queries value: HKLM\software\policies\microsoft\internet explorer\security[disablesecuritysettingscheck]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[autodetect]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1a10]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation[explorer.exe]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[2101]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[typeahead]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\advanced[typeahead]
Queries value: HKCU\appevents\schemes\apps\.default\.default\.current[]
Queries value: HKCU\appevents\schemes\apps\.default\.default\.current[default flags]
Queries value: HKLM\system\currentcontrolset\control\timezoneinformation[bias]
Queries value: HKLM\system\currentcontrolset\control\timezoneinformation[standardname]
Queries value: HKLM\system\currentcontrolset\control\timezoneinformation[standardbias]
Queries value: HKLM\system\currentcontrolset\control\timezoneinformation[standardstart]
Queries value: HKLM\system\currentcontrolset\control\timezoneinformation[daylightname]
Queries value: HKLM\system\currentcontrolset\control\timezoneinformation[daylightbias]
Queries value: HKLM\system\currentcontrolset\control\timezoneinformation[daylightstart]

Queries value:
HKLM\system\currentcontrolset\control\timezoneinformation[timezonekeyname]
Queries value:
HKLM\system\currentcontrolset\control\timezoneinformation[dynamicdaylighttimedisabled]
Queries value:
HKLM\system\currentcontrolset\control\timezoneinformation[activetimebias]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
Queries value: HKLM\software\policies\microsoft\windows\system[gpsvcdebuglevel]
Queries value:
HKLM\system\currentcontrolset\services\w32time\parameters[servicedllunloadonstop]
Queries value: HKLM\system\currentcontrolset\services\eventlog\security[type]
Queries value: HKLM\system\currentcontrolset\services\eventlog\security[filemax]
Queries value: HKLM\system\currentcontrolset\services\eventlog\security[filecounter]
Queries value: HKLM\system\currentcontrolset\services\eventlog\security[buffersize]
Queries value: HKLM\system\currentcontrolset\services\eventlog\security[minbuffers]
Queries value: HKLM\system\currentcontrolset\services\eventlog\security[maxbuffers]
Queries value: HKLM\system\currentcontrolset\services\eventlog\security[latency]
Queries value: HKLM\system\currentcontrolset\control\terminal
server\winstations[selfsignedcertificate]
Queries value: HKLM\system\currentcontrolset\control\terminal
server\winstations[selfsignedcertstore]
Queries value: HKLM\system\currentcontrolset\services\eventlog\security[clocktype]
Queries value: HKLM\system\currentcontrolset\services\eventlog\security[level]
Queries value: HKLM\system\currentcontrolset\services\eventlog\security[controlguid]
Queries value: HKLM\system\currentcontrolset\services\eventlog\security[maxsize]
Queries value: HKLM\system\currentcontrolset\services\eventlog\security[maxsizeupper]
Queries value: HKLM\system\currentcontrolset\services\eventlog\security[retention]
Queries value:
HKLM\system\currentcontrolset\services\eventlog\security[autobackuplogfiles]
Queries value: HKLM\software\microsoft\systemcertificates\remote
desktop\certificates\d30806d4a0b6f6f6a90d99a889009077e446491f[blob]
Queries value: HKLM\system\currentcontrolset\services\eventlog\security[file]
Queries value: HKLM\system\currentcontrolset\services\eventlog\security[flags]
Queries value: HKLM\system\currentcontrolset\services\eventlog\security[filterid]
Queries value: HKLM\system\currentcontrolset\services\eventlog\security[isolation]
Queries value:
HKLM\system\currentcontrolset\services\eventlog\security[owningpublisher]
Queries value: HKLM\system\currentcontrolset\services\eventlog\security[customsd]
Queries value: HKLM\system\currentcontrolset\control\terminal
server\winstations[templatecertificate]
Queries value: HKLM\software\policies\microsoft\windows nt\terminal
services[certtemplatename]
Queries value: HKLM\system\currentcontrolset\control\terminal
server\winstations\console[fmonitorcertificate]
Queries value: HKLM\system\currentcontrolset\control\terminal
server\winstations\console[sslcertificatesha1hash]
Queries value: HKLM\system\currentcontrolset\control\terminal server\winstations\eh-
tcp[fmonitorcertificate]
Queries value: HKLM\system\currentcontrolset\control\terminal server\winstations\rdp-
tcp[fmonitorcertificate]
Queries value: HKLM\system\currentcontrolset\control\terminal server\winstations\rdp-
tcp[sslcertificatesha1hash]
Queries value: HKLM\system\currentcontrolset\control\terminal
server\winstations[certrefreshinterval]
Queries value: HKLM\system\currentcontrolset\services\eventlog\security[keywordslower]
Queries value: HKLM\system\currentcontrolset\services\eventlog\security[keywordsupper]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54849625-5478-4994-a5ba-
3e3b0328c30d}\channelreferences[count]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54849625-5478-4994-a5ba-
3e3b0328c30d}\channelreferences\0[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54849625-5478-4994-a5ba-
3e3b0328c30d}\channelreferences\0[flags]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54849625-5478-4994-a5ba-
3e3b0328c30d}\channelreferences\0[id]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]

Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
Queries value:
HKCU\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
Queries value: HKU\.default\control panel\international[localename]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[type]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[filemax]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[filecounter]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[buffersize]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[minbuffers]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[maxbuffers]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[latency]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[clocktype]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[level]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[controlguid]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[maxsize]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[maxsizeupper]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[retention]
Queries value:
HKLM\system\currentcontrolset\services\eventlog\system[autobackuplogfiles]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[file]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[flags]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[filterid]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[owningpublisher]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[customsd]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a68ca8b7-004f-d7b6-a698-
07e2de0f1f5d}\channelreferences[count]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a68ca8b7-004f-d7b6-a698-
07e2de0f1f5d}\channelreferences\0[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a68ca8b7-004f-d7b6-a698-
07e2de0f1f5d}\channelreferences\0[flags]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a68ca8b7-004f-d7b6-a698-
07e2de0f1f5d}\channelreferences\0[id]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{06edcfeb-0fd0-4e53-acca-
a6f8bbf81bcb}\channelreferences[count]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{06edcfeb-0fd0-4e53-acca-
a6f8bbf81bcb}\channelreferences\0[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{06edcfeb-0fd0-4e53-acca-
a6f8bbf81bcb}\channelreferences\0[flags]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{06edcfeb-0fd0-4e53-acca-
a6f8bbf81bcb}\channelreferences\0[id]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
Queries value:
HKLM\system\currentcontrolset\services\netlogon\parameters[expecteddialupdelay]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietldversionlow]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietldversionhigh]
Queries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[{aeba21fa-782a-4a90-978d-b72164c80120}]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[privacyadvanced]
Queries value: HKLM\software\microsoft\reliability analysis\wmi[wmienable]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[f52ac1cc-b92d-4d8e-
8cf5-699ca40a73d2]
Queries value:
HKLM\system\currentcontrolset\control\diagnostics\performance[disablediagnostictracing]
Queries value:
HKLM\system\currentcontrolset\control\diagnostics\performance[activeshutdowndcl]
Queries value:
HKLM\software\policies\microsoft\windows\system[copyfilebufferedsynchronousio]
Queries value: HKLM\software\policies\microsoft\windows\system[copyfilechunksize]
Queries value: HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\boot[postboot_busythreshold]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\boot[postboot_timetoaccumulate_sec]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\boot[hardthresholds_critserviceslist]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\boot[mindelaypercentagetoidentify]

Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\boot[numinitialbootstoignore]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\systemboot[distantsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\systemboot[recentsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\systemboot[currentsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\systemboot[distantquorum]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\systemboot[recentquorum]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\systemboot[currentquorum]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\systemboot[flatthresholdingconfig]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot[distantsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot[recentsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot[currentsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot[distantquorum]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot[recentquorum]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot[currentquorum]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot[flatthresholdingconfig]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[distantsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[recentsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[currentsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[distantquorum]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[recentquorum]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[currentquorum]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[numinitialshutdownstoignore]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[flatthresholdingconfig]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[shutdownminorthreshold_sec]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[shutdownmajorthreshold_sec]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[logoffminorthreshold_sec]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[logoffmajorthreshold_sec]
Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a7098685]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[messagefilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[categorymessagefile]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[resourcefilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[parameterfilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[helplink]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[categorycount]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[type]
Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[channelaccess]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[latency]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[keywordslower]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[keywordsupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[channelaccess]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[keywordslower]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-

performance/diagnostic/loopback[keywordsupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[channelaccess]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\boot[postbootminorthreshold_sec]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\boot[postbootmajorthreshold_sec]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\boot[bootminorthreshold_sec]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\boot[bootmajorthreshold_sec]
Queries value: HKLM\system\currentcontrolset\services\nnetsecl[imagepath]
Queries value: HKLM\system\currentcontrolset\services\themes[imagepath]
Queries value: HKLM\system\currentcontrolset\services\themes\parameters[servicedll]
Queries value: HKLM\system\currentcontrolset\services\profsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\profsvc\parameters[servicedll]
Queries value: HKLM\system\currentcontrolset\services\gpsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\gpsvc\parameters[servicedll]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
Queries value:
HKLM\software\microsoft\windows\currentversion\reliability[timestampinterval]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0063715b-eeda-4007-9429-ad526f62696e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{01090065-b467-4503-9b28-533766761087}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{01578f96-c270-4602-ade0-578d9c29fc0c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{017247f2-7e96-11dc-8314-0800200c9a66}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{017ba13c-9a55-4f1f-8200-323055aac810}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{01979c6a-42fa-414c-b8aa-eee2c8202018}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{02012a8a-adf5-4fab-92cb-ccb7bb3e689a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{030f2f57-abd0-4427-bcf1-3a3587d7dc7d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{04268430-d489-424d-b914-0cff741d6684}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{04d66358-c4a1-419b-8023-23b73902de2c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{05921578-2261-42c7-a0d3-26ddbce6c50d}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{059c3e04-5535-4929-85e1-93030e78f47b}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{05d7b0f0-2121-4eff-bf6b-ed3f69b894d7}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{06184c97-5201-480e-92af-3a3626c5b140}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{06edcfeb-0fd0-4e53-acca-a6f8bbf81bcb}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{07de7879-1c96-41ce-afbd-c659a0e8e643}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{08466062-aed4-4834-8b04-cddb414504e5}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0888e5ef-9b98-4695-979d-e92ce4247224}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{093da50c-0bb9-4d7d-b95c-3bb9fcda5ee8}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{09608c12-c1da-4104-a6fe-b959cf57560a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{099614a5-5dd7-4788-8bc9-e29f43db28fc}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{09ec9687-d7ad-40ca-9c5e-78a04a5ae993}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0a88862d-20a3-4c1f-b76f-162c55adbf93}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0bd3506a-9030-4f76-9b88-3e8fe1f7cfb6}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0c478c5b-0351-41b1-8c58-4a6737da32e3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0d4fdc09-8c27-494a-bda0-505e4fd8adae}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0d759f0f-cff9-4902-8867-eb9e29d7a98b}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0dd4d48e-2bbf-452f-a7ec-ba3dba8407ae}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0f177893-4a9c-4709-b921-f432d67f43d5}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0f67e49f-fe51-4e9f-b490-6f2948cc6027}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{11a377e3-be1e-4ee7-abda-81c6eda62e71}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{11a75546-3234-465e-bec8-2d301cb501ac}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{122ee297-bb47-41ae-b265-1ca8d1886d40}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{127e0dc5-e13b-4935-985e-78fd508b1d80}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{13480a22-d79f-4334-9d32-aa239398ad3c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{134ea407-755d-4a93-b8a6-f290cd155023}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{13b197bd-7cee-4b4e-8dd0-59314ce374ce}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1418ef04-b0b4-4623-bf7e-

d74ab47bbdaa}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{155cb334-3d7f-4ff1-b107-df8afc3c0363}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{15a7a4f8-0072-4eab-abad-f98a4d666aed}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{15ca44ff-4d7a-4baa-bba5-0998955e531e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{17d6e590-f5fe-11dc-95ff-0800200c9a66}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{17e92e2a-3d08-413e-baeb-a79a262bf486}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{17f14a23-551d-40cc-a086-e4194d64ed4c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{18f4a5fd-fd3b-40a5-8fc2-e5d261c5d02e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{192ede41-9175-4c86-ac02-9d003c9d43ab}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{199fe037-2b82-40a9-82ac-e1d46c792b99}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{19d2c934-ee9b-49e5-aaeb-9cce721d2c65}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1a396961-5f3c-4c71-8310-44c653c0bf8a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1a772f65-be1e-4fc6-96bb-248e03fa60f5}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1a9443d4-b099-44d6-8eb1-829b9c2fe290}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1b562e86-b7aa-4131-badc-b6f3a001407e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1b8b402d-78dc-46fb-bf71-46e64aedf165}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1be1a88d-8e34-4170-9123-f503375bbcef}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1c95126e-7eea-49a9-a3fe-a378b03ddb4d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1d75856d-36a7-4ecb-a3f5-b13152222d29}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1db28f2e-8f80-4027-8c5a-a11f7f10f62d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1edeee53-0afe-4609-b846-d8c0b2075b1f}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1f678132-5938-4686-9fdc-c8ff68f15c85}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1f84007d-19ce-4b15-9e81-8a3dd8eb9ecb}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{206f6dea-d3c5-4d10-bc72-989f03c8b84b}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{21b7c16e-c5af-4a69-a74a-7245481c1b97}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{22b6d684-fa63-4578-87c9-effcbe6643c7}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{22fb2cd6-0e7b-422b-a0c7-2fad1fd0e716}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{239cfb83-cbb7-4bbc-a02e-9bdb496aa7c2}[]
Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{271c5228-c3fe-4e47-831f-48c3652ce5ac}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{272a979b-34b5-48ec-94f5-7225a59c85a0}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{27a8c1e2-eb19-463e-8424-b399df27a216}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{28aa95bb-d444-4719-a36f-40462168127e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2992e9cf-4f99-48f5-a0b6-b99b11cd387d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{29d13147-1c2e-48ec-9994-e29dfe496eb3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2a274310-42d5-4019-b816-e4b8c7abe95c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2d318b91-e6e7-4c46-bd04-bfe6db412cf9}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2e35aaeb-857f-4beb-a418-2e6c0e54d988}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2ed6006e-4729-4609-b423-3ee7bcd678ef}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2f07e2ee-15db-40f1-90ef-9d7ba282188a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2fd7a9a5-b1a1-4fc7-b95c-c32fed818f30}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2ff3e6b7-cb90-4700-9621-443f389734ed}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{30336ed4-e327-447c-9de0-51b652c86108}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{314b2b0d-81ee-4474-b6e0-c2aaec0ddbde}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{314de49f-ce63-4779-ba2b-d616f6963a88}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{319122a9-1485-4e48-af35-7db2d93b8ad2}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{31f60101-3703-48ea-8143-451f8de779d2}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3239eb6f-c7fc-4953-aa15-646829a4ca4c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{331c3b3a-2005-44c2-ac5e-77220c37d6b4}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{355c44fe-0c8e-4bf8-be28-8bc7b5a42720}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{35ac6ce8-6104-411d-976c-877f183d2d32}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3663a992-84be-40ea-bba9-90c7ed544222}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{36c23e18-0e66-11d9-bbeb-505054503030}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{37945dc2-899b-44d1-b79c-dd4a9e57ff98}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3aa52b8b-6357-4c18-a92e-b53fb177853b}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3c6c422b-019b-4f48-b67b-f79a3fa8b4ed}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3cb2a168-fe19-4a4e-bdad-dcf422f13473}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3cb40aaa-1145-4fb8-b27b-7e30f0454316}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3cc2d4af-da5e-4ed4-bcbe-3cf995940483}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3df0c2c1-5a04-4966-9790-df6ef0ccde9c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3f7b2f99-b863-4045-ad05-f6afb62e7af1}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3f9e07bd-0e26-4241-a5a5-28cafa150a75}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{40ab57c2-1c53-4df9-9324-ff7cf898a02c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{40ae003c-6f3d-4590-ae1c-0e8be526b50f}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4214dcd2-7c33-4f74-9898-719ccceec20f}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{422088e6-cd0c-4f99-bd0b-6985fa290bdf}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{43d1a55c-76d6-4f7e-995c-64c711e5cafe}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{43e63da5-41d1-4fbf-aded-1bbed98fdd1d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{46098845-8a94-442d-9095-366a6bcfefa9}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{49c2c27c-fe2d-40bf-8c4e-c3fb518037e7}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4a933674-fb3d-4e8d-b01d-17ee14e91a3e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4b7eac67-fc53-448c-a49d-7cc6db524da7}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ba32972-6fc5-488a-8368-5da620d05127}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4cb314df-c11f-47d7-9c04-65fb0051561b}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4cec9c95-a65f-4591-b5c4-30100e51d870}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4edbe902-9ed3-4cf0-93e8-b8b5fa920299}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ee76bd8-3cf4-44a0-a0ac-3937643e37a3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ef850d8-bf30-4e64-a917-ee21b9be1f0a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4f768be8-9c69-4bbc-87fc-95291d3f9d0c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4fba1227-f606-4e5f-b9e8-fab9ab5740f3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4fcbf664-a33a-4652-b436-9d558983d955}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{50b3e73c-9370-461d-bb9f-26f32d68887d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{50bd1bfd-936b-4db3-86be-e25b96c25898}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{51480c1a-90aa-416e-98fd-4c11f735349b}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5322d61a-9efa-4bc3-a3f9-

14be95c144f8}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{538cbbad-4877-4eb2-b26e-7caee8f0f8cb}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54164045-7c50-4905-963f-e5bc1eef0cca}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5444519f-2484-45a2-991e-953e4b54c8e0}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{546549be-9d63-46aa-9154-4f6eb9526378}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54732ee5-61ca-4727-9da1-10be5a4f773d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54849625-5478-4994-a5ba-3e3b0328c30d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54d5ac20-e14f-4fda-92da-ebf7556ff176}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54ffd262-99fe-4576-96e7-1adb500370dc}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{57e0b31d-de8c-4181-bcd1-f70e880b49fc}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5857d6ca-9732-4454-809b-2a87b70881f8}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{588c5c5a-ffc5-44a2-9a7f-d5e8dbe6efd7}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{588cd2e4-a5b0-492d-a59b-f6dd3e7681c6}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5a24fcdb-1cf3-477b-b422-ef4909d51223}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5b004607-1087-4f16-b10e-979685a8d131}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5b0a651a-8807-45cc-9656-7579815b6af0}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5b93cdfa-5f51-45e0-9fde-296983129e6c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5bbca4a8-b209-48dc-a8c7-b23d3e5216fb}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5c8bb950-959e-4309-8908-67961a1205d5}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5c9be3e0-3593-4dcd-8f6d-63840923ffee}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5d674230-ca9f-11da-a94d-0800200c9a66}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5d896912-022d-40aa-a3a8-4fa5515c76d7}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5d9e0020-3761-4f36-90c8-38ce6511bd12}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5ec13d8e-4b3f-422e-a7e7-3121a1d90c7a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5f92bc59-248f-4111-86a9-e393e12c6139}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{606a6a38-70ec-4309-b3a3-82ff86f73329}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{614696c9-85af-4e64-b389-d2c0db4ff87b}[]
Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{617853d6-728b-4b59-8a78-c3a9a5eade92}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{61f044af-9104-4ca5-81ee-cb6c51bb01ab}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{63b530f8-29c9-4880-a5b4-b8179096e7b8}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{63d1e632-95cc-4443-9312-af927761d52a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{63d2bb1d-e39a-41b8-9a3d-52dd06677588}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{651df93b-5053-4d1e-94c5-f6e6d25908d0}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{65d341f3-baaa-4c6e-8b20-23d4f1574004}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{65d99466-7a8e-489c-b8e1-962bc945031e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6600e712-c3b6-44a2-8a48-935c511f28c8}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{66a5c15c-4f8e-4044-bf6e-71d896038977}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{676f167f-f72c-446e-a498-eda43319a5e3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67bd1fef-afb2-458d-bcde-3758beb84dec}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67fe2216-727a-40cb-94b2-c02211edb34a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6863e644-dd5d-43a2-a8b5-7a81b46672e6}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{699e309c-e782-4400-98c8-e21d162d7b7b}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6a1f2b00-6a90-4c38-95a5-5cab3b056778}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6a2dc7c1-930a-4fb5-bb44-80b30aebed6c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6a502821-ab44-40c8-b32f-37315d9d52e0}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6ad52b32-d609-4be9-ae07-ce8dae937e39}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6addabf4-8c54-4eab-bf4f-fbef61b62eb0}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6b1ffe48-5b1e-4793-9f7f-ae926454499d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6b4db0bc-9a3d-467d-81b9-a84c6f2f3d40}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6b93bf66-a922-4c11-a617-cf60d95c133d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6ba132c4-da49-415b-a7f4-31870dc9fe25}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6bba3851-2c7e-4dea-8f54-31e5afd029e3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6c260f2c-049a-43d8-bf4d-d350a4e6611a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6d8a3a60-40af-445a-98ca-99359e500146}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6e400999-5b82-475f-b800-cef6fe361539}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6eb8db94-fe96-443f-a366-5fe0cee7fb1c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6ece3302-fee1-4ea9-8b88-086d459ed976}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{70eb4f03-c1de-4f73-a051-33d13d5413bd}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{712abb2d-d806-4b42-9682-26da01d8b307}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{719be4ed-e9bc-4dd8-a7cf-c85ce8e4975d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7237fff9-a08a-4804-9c79-4a8704b70b87}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7288c9f8-d63c-4932-a345-89d6b060174d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{728b8c72-0f0f-4071-9bcc-27cb3b6dacbe}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{72d211e1-4c54-4a93-9520-4901681b2271}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{73370bd6-85e5-430b-b60a-fea1285808a7}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{73e9c9de-a148-41f7-b1db-4da051fdc327}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{741fc222-44ed-4ba7-98e3-f405b2d2c4b4}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7426a56b-e2d5-4b30-bdef-b31815c1a74a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{747ef6fd-e535-4d16-b510-42c90f6873a1}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{74b4a4b1-2302-4768-ac5b-9773dd456b08}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{74b655a2-8958-410e-80e2-3457051b8dff}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{74c2135f-cc76-45c3-879a-ef3bb1eeaf86}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-0870-49e5-bdce-9d7028279489}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-0936-4a55-9d26-5f298f3180bf}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-0cc6-49da-8cd9-8903a5222aa0}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-77b8-4ba8-9474-4f4a9db2f5c6}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-8670-4eb6-b535-3b9d6bb222fd}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-997f-49cf-b49f-ecc50184b75d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-c8ae-4f93-9ca1-683a53e20cb6}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-d017-4d0f-93ab-0b4f86579164}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75f48521-4131-4ac3-9887-65473224fcb2}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{777ba8fe-2498-4875-933a-3067de883070}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{78168022-eca5-41e8-9e17-

e8c7fd77aae1}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7839bb2a-2ea3-4eca-a00f-b558ba678bec}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7a67066e-193f-4d3a-82d3-322fee5259de}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7b563579-53c8-44e7-8236-0f87b9fe6594}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7b6bc78c-898b-4170-bbf8-1a469ea43fc5}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7b7838a3-6562-4269-bb7a-97b0d9593882}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7bb5af18-cb16-4007-b813-9d88e9d6f8ef}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7bfcf102-7378-431c-9284-0b968258991a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7c314e58-8246-47d1-8f7a-4049dc543e0b}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7d29d58a-931a-40ac-8743-48c733045548}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7d44233d-3055-4b9c-ba64-0d47ca40a232}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7d5387b0-cbe0-11da-a94d-0800200c9a66}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7d7b0c39-93f6-4100-bd96-4dda859652c5}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7da4fe0e-fd42-4708-9aa5-89b77a224885}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7dd42a49-5329-4832-8dfd-43d979153a88}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7eafcf79-06a7-460b-8a55-bd0a0c9248aa}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7f2bd991-ae93-454a-b219-0bc23f02262a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7f912b92-21ad-496e-b97a-88622a72bc42}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7f9d83de-8abb-457f-98e8-4ad161449ecc}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{802ec45a-1e99-4b83-9920-87c98277ba9d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8085cb91-900e-4d15-a7d1-921ddce641d8}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8115579e-2bea-4c9e-9ab1-821cc2c98ab0}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{820a42d8-38c4-465d-b64e-d7d56ea1d612}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{835b79e2-e76a-44c4-9885-26ad122d3b4d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8360bd0f-a7dc-4391-91a7-a457c5c381e4}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{83ed54f0-4d48-4e45-b16e-726ffd1fa4af}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{84051b98-f508-4e54-82fa-8865c697c3b1}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8429e243-345b-47c1-8a91-2c94caf0daab}[]
Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8443ccb7-feb0-4b8d-8e28-8d4c7cb814e8}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{85fe7609-ff4a-48e9-9d50-12918e43e1da}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{86133982-63d7-4741-928e-ef1349b80219}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{869fb599-80aa-485d-bca7-db18d72b7219}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{86efff39-2bdd-4efd-bd0b-853d71b2a9dc}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{87d476fe-1a0f-4370-b785-60b028019693}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8939299f-2315-4c5c-9b91-abb86aa0627d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{899daace-4868-4295-afcd-9eb8fb497561}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{89a2278b-c662-4aff-a06c-46ad3f220bca}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{89b1e9f0-5aff-44a6-9b44-0a07a7ce5845}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8a93b54b-c75a-49b5-a5be-9060715b1a33}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8c63b5a5-b484-4381-892d-edd424582df7}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8c9dd1ad-e6e5-4b07-b455-684a9d879900}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8ce93926-bdae-4409-9155-2fe4799ef4d3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{914ed502-b70d-4add-b758-95692854f8a3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{91f42016-0b4e-4a4b-9bbb-825d06cbed35}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{91f5fb12-fdea-4095-85d5-614b495cd9de}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{92ae46d7-6d9c-4727-9ed5-e49af9c24cbf}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9363ccd9-d429-4452-9adb-2501e704b810}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{93c05d69-51a3-485e-877f-1806a8731346}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{945a8954-c147-4acd-923f-40c45405a658}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9485fa1e-23cd-49a1-84e3-11d8bc550cb7}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{952773bf-c2b7-49bc-88f4-920744b82c43}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{95353826-4fbe-41d4-9c42-f521c6e86360}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9580d7dd-0379-4658-9870-d5be7d52d6de}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{959f1fac-7ca8-4ed1-89dc-cdfa7e093cb0}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{968f313b-097f-4e09-9cdd-bc62692d138b}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{96ac7637-5950-4a30-b8f7-e07e8e5734c1}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{96f4a050-7e31-453c-88be-9634f4e02139}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{973143dd-f3c7-4ef5-b156-544ac38c39b6}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{98583af0-fc93-4e71-96d5-9f8da716c6b8}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{98bf1cd3-583e-4926-95ee-a61bf3f46470}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{98e6cfcb-ee0a-41e0-a57b-622d4e1b30b1}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{99806515-9f51-4c2f-b918-1eae407aa8cb}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9988748e-c2e8-4054-85f6-0c3e1cad2470}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9b307223-4e4d-4bf5-9be8-995cd8e7420b}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9b6123dc-9af6-4430-80d7-7d36f054fb9f}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9c205a39-1250-487d-abd7-e831c6290539}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9d55b53d-449b-4824-a637-24f9d69aa02f}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9db0fdb5-3b21-440e-a94b-63738a4be5de}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9e03f75a-bcbe-428a-8f3c-d46f2a444935}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9e3b3947-ca5d-4614-91a2-7b624e0e7244}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9e6ae157-d9f7-47e5-8c6d-b17bb6c82a27}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9e95e4d0-4cb4-4b5d-a936-c972d7d08d90}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9f0c4ea8-ec01-4200-a00d-b9701cbea5d8}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9f650c63-9409-453c-a652-83d7185a2e83}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a0c1853b-5c40-4b15-8766-3cf1c58f985a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a0e3d8ea-c34f-4419-a1db-90435b8b21d0}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a319d300-015c-48be-acdb-47746e154751}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a3e1697b-a12c-46b9-84d1-7ffe73c4b678}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a402fe09-da6e-45f2-82af-3cb37170ee0c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a50b09f8-93eb-4396-84c9-dc921259f952}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a615acb9-d5a4-4738-b561-1df301d207f8}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a68ca8b7-004f-d7b6-a698-07e2de0f1f5d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a6ad76e3-867a-4635-91b3-4904ba6374d7}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a6f32731-9a38-4159-a220-

3d9b7fc5fe5d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a7364e1a-894f-4b3d-a930-2ed9c8c4c811}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a7975c8f-ac13-49f1-87da-5a984a4ab417}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a8106e5c-293a-4cd0-9397-2e6fac7f9749}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a82fda5d-745f-409c-b0fe-18ae0678a0e0}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a8a1f2f6-a13a-45e9-b1fe-3419569e5ef2}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a97524f6-064c-4c4e-b74b-1acc87c3700d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{aabf8b86-7936-4fa2-acb0-63127f879dbf}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{aaf44901-5c64-4014-8b6c-a80813937293}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ab0d8ef9-866d-4d39-b83f-453f3b8f6325}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{abce23e7-de45-4366-8631-84fa6c525952}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ac43300d-5fcc-4800-8e99-1bd3f85f0320}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ad5162d8-daf0-4a25-88a7-01cbeb33902e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ad8aa069-a01b-40a0-ba40-948d1d8dedc5}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ae4bd3be-f36f-45b6-8d21-bdd6fb832853}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{aea1b4fa-97d1-45f2-a64c-4d69fffd92c9}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{af0a5a6d-e009-46d4-8867-42f2240f8a72}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{af2e340c-0743-4f5a-b2d3-2f7225d215de}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{af9cc194-e9a8-42bd-b0d1-834e9cfab799}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b03d4051-3564-4e93-93db-3c34f1b5b503}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b059b83f-d946-4b13-87ca-4292839dc2f2}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b1bebb9a-24aa-4b83-9e4a-38c2a9a44377}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b1c94ed9-ac9b-410e-aa48-4ffc5e45f4e3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b1f90b27-4551-49d6-b2bd-dfc6453762a6}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b2a40f1f-a05a-4dfd-886a-4c4f18c4334c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b3eee223-d0a9-40cd-adfc-50f1888138ab}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b44aec44-38f4-4b59-8df3-10306abf19b2}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b5fd844a-01d4-4b10-a57f-58b13b561582}[]
Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b65471e1-019d-436f-bc38-e15fa8e87f53}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b675ec37-bdb6-4648-bc92-f3fdc74d3ca2}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b92cf7fd-dc10-4c6b-a72d-1613bf25e597}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b977cf02-76f6-df84-cc1a-6a4b232322b6}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b98f0db6-26e2-4a66-89fc-32a9a6a9af61}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b9da9fe6-ae5f-4f3e-b2fa-8e623c11dc75}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ba093605-3909-4345-990b-26b746adee0a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bbe94f36-f8dc-4c33-8227-81602b7a3d53}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bc2eeeec-b77a-4a52-b6a4-dffb1b1370cb}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bc97b970-d001-482f-8745-b8d7d5759f99}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bd12f3b8-fc40-4a61-a307-b7a013a069c1}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bd2d1dae-d678-4e10-9667-21cba2aa70c3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bd2f4252-5e1e-49fc-9a30-f3978ad89ee2}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bdb462fc-a297-49a2-bf2e-4f1809e12abc}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{be69781c-b63b-41a1-8e24-a4fc7b3fc498}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{be932b00-0f8e-4386-ab89-873f7d0274aa}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bf406804-6afa-46e7-8a48-6c357e1d6d61}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c02afc2b-e24e-4449-ad76-bcc2c2575ead}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c06ed57a-a7bd-42d7-b5ff-77a9dec5732d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c100becc-d33a-4a4b-bf23-bbef4663d017}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c100becf-d33a-4a4b-bf23-bbef4663d017}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c26c4f3c-3f66-4e99-8f8a-39405cfed220}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c2fa0899-8a10-412b-a42e-9e5b284a2437}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c4636a1e-7986-4646-bf10-7bc3b4a76e8e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c514638f-7723-485b-bcfc-96565d735d4a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c6bf6832-f7bd-4151-ac21-753ce4707453}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c76baa63-ae81-421c-b425-340b4b24157f}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c7bde69a-e1e0-4177-b6ef-283ad1525271}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c882ff1d-7585-4b33-b135-95c577179137}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c88a4ef5-d048-4013-9408-e04b7db2814a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c89b991e-3b48-49b2-80d3-ac000dfc9749}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c8f7689f-3692-4d66-b0c0-9536d21082c9}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c914f0df-835a-4a22-8c70-732c9a80c634}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c91ef675-842f-4fcf-a5c9-6ea93f2e4f8b}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c9bdb4eb-9287-4c8e-8378-6896f0d1c5ef}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ca4e628d-8567-4896-ab6b-835b221f373f}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ca5ba219-c0d4-4efa-9ceb-72aff92672b0}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cab2b8a5-49b9-4eec-b1b0-fac21da05a3b}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cad2d809-03d9-4f46-9cf4-72aa4f04b6b9}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cb070027-1534-4cf3-98ea-b9751f508376}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cb587ad1-cc35-4ef1-ad93-36cc82a2d319}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cbda4dbf-8d5d-4f69-9578-be14aa540d22}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cd032e15-15ad-4da4-afc6-03bf83516195}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cdc05e28-c449-49c6-b9d2-88cf761644df}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cdead503-17f5-4a3e-b7ae-df8cc2902eb9}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ce20d1c3-a247-4c41-bcb8-3c7f52c8b805}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ce8dee0b-d539-4000-b0f8-77bed049c590}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cf3f502e-b40d-4071-996f-00981edf938e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfaa5446-c6c4-4f5c-866f-31c9b55b962d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d02a9c27-79b8-40d6-9b97-cf3f8b7b5d60}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d1bc9aff-2abf-4d71-9146-ecb2a986eb85}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d1d93ef7-e1f2-4f45-9943-03d245fe6c00}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d4263c98-310c-4d97-ba39-b55354f08584}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d53270e3-c8cf-4707-958a-dad20c90073c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d5c25f9a-4d47-493e-9184-40dd397a004d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d6f68875-cdf5-43a5-a3e3-

53ffd683311c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d8975f88-7ddb-4ed0-91bf-3adf48c48e0c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dab065a9-620f-45ba-b5d6-d6bb8efedee9}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dab3b18c-3c0f-43e8-80b1-e44bc0dad901}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{db00dfb6-29f9-4a9c-9b3b-1f4f9e7d9770}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dbe9b383-7cf3-4331-91cc-a3cb16a3b538}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dd5ef90a-6398-47a4-ad34-4dcecdef795f}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dd70bc80-ef44-421b-8ac3-cd31da613a4e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dd85457f-4e2d-44a5-a7a7-6253362e34dc}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{de513a55-c345-438b-9a74-e18cac5c5cc5}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{de7b24ea-73c8-4a09-985d-5bdadcfa9017}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dea07764-0790-44de-b9c4-49677b17174f}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ded165cf-485d-4770-a3e7-9c5f0320e80c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{df32a572-0b4b-44be-b09b-72084fdbf879}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e01b1a7c-c5c9-4e67-99a9-5e85acfb2e10}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e04fe2e0-c6cf-4273-b59d-5c97c9c374a4}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e0a40b26-30c4-4656-bc9a-74a5c3a0b2ec}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e104fb41-6b04-4f3a-b47d-f0df2f02b954}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e1dd7e52-621d-44e3-a1ad-0370c2b25946}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e23b33b0-c8c9-472c-a5f9-f2bdfea0f156}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e2816346-87f4-4f85-95c3-0c79409aa89d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e4480490-85b6-11dd-ad8b-0800200c9a66}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e46eead8-0c54-4489-9898-8fa79d059e0e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e4d53f84-7de3-11d8-9435-505054503030}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e53c6823-7bb8-44bb-90dc-3f86090d48a6}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e595f735-b42a-494b-afcd-b68666945cd3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e5ba83f6-07d0-46b1-8bc7-7e669a1d31dc}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e6307a09-292c-497e-aad6-498f68e2b619}[]
Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e670a5a2-ce74-4ab4-9347-61b815319f4c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e7558269-3fa5-46ed-9f4d-3c6e282dde55}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e7ef96be-969f-414f-97d7-3ddb7b558ccc}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e8316a2d-0d94-4f52-85dd-1e15b66c5891}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e837619c-a2a8-4689-833f-47b48ebd2442}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e856c26a-e105-4683-a948-6920dcc42e45}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e978f84e-582d-4167-977e-32af52706888}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eb3deb18-d1de-4897-8502-a230ad03db8a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ed6b3ba8-95b2-4cf5-a317-d4af7003884c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{edd08927-9cc4-4e65-b970-c2560fb5c289}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ee4f43b5-03eb-41d2-a28c-ba8bee529247}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-82fd4940b820}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ef1cc15b-46c1-414e-bb95-e76b077bd51e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f0db7ef8-b6f3-4005-9937-feb77b9e1b43}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f230d19a-5d93-47d9-a83f-53829edfb8df}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f2c628ae-d26c-4352-9c45-74754e1e2f9f}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f3c5e28e-63f6-49c7-a204-e48a1bc4b09d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f3f14ff3-7b80-4868-91d0-d77e497b025e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f404b94e-27e0-4384-bfe8-1d8d390b0aa3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f4aed7c7-a898-4627-b053-44a7caa12fcd}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f5344219-87a4-4399-b14a-e59cd118abb8}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f557ace2-bcf8-4994-8e4b-42368a6f078a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f5d05b38-80a6-4653-825d-c414e4ab3c68}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f61cefc0-aa2e-11da-a746-0800200c9a66}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f6da35ce-d312-41c8-9828-5a2e173c91b6}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f82fb576-e941-4956-a2c7-a0cf83f6450a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f997cd11-0fc9-4ab4-acba-bc742a4c0dd3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{fbcfac3f-8459-419f-8e48-1f0b49cdb85e}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{fc3bc8a7-2f61-449c-a8b4-22ac22058f92}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{fc65ddd8-d6ef-4962-83d5-6e5cfe9ce148}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{fc6f77dd-769a-470e-bcf9-1b6555a118be}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{fd771d53-8492-4057-8e35-8c02813af49b}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ffdb9886-80f3-4540-aa8b-b85192217ddf}[]
Queries value:
HKLM\system\currentcontrolset\services\eventlog\system\eventlog[providerguid]
Queries value:
HKLM\system\currentcontrolset\services\eventlog\system\eventlog[eventmessagefile]
Queries value:
HKLM\system\currentcontrolset\services\eventlog\system\eventlog[categorymessagefile]
Queries value:
HKLM\system\currentcontrolset\services\eventlog\system\eventlog[resourcefilename]
Queries value:
HKLM\system\currentcontrolset\services\eventlog\system\eventlog[parametermessagefile]
Queries value:
HKLM\system\currentcontrolset\services\eventlog\system\eventlog[helplink]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system\eventlog[enabled]
Queries value:
HKLM\system\currentcontrolset\services\eventlog\system\eventlog[categorycount]
Queries value: HKLM\system\currentcontrolset\services\bits\parameters[servicedll]
Queries value: HKLM\system\currentcontrolset\services\bits\parameters[servicemanifest]
Queries value: HKLM\system\currentcontrolset\services\bits\parameters[servicemain]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[4a8aaa94-cfc4-46a7-8e4e-17bc45608f0a]
Queries value: HKLM\software\microsoft\windows\currentversion\bits[logfilesize]
Queries value: HKLM\software\microsoft\windows\currentversion\bits[logfileflags]
Queries value: HKLM\software\microsoft\windows\currentversion\bits[logfileminmemory]
Queries value: HKLM\system\currentcontrolset\services\bits\performance[first counter]
Queries value: HKLM\system\currentcontrolset\services\bits\performance[first help]
Queries value: HKLM\system\currentcontrolset\services\bits\performance[last counter]
Queries value: HKLM\system\currentcontrolset\services\bits\performance[last help]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-

a9dd-070d1d495d97}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[initfolderhandler]
Queries value:
HKLM\system\currentcontrolset\control\backuprestore\filesnottobackup[bits_metadata]
Queries value:
HKLM\software\microsoft\windows\currentversion\bits[jobinactivitytimeout]
Queries value: HKLM\software\microsoft\windows\currentversion\bits[timequantalength]
Queries value:
HKLM\software\microsoft\windows\currentversion\bits[jobnoprogresstimeout]
Queries value:
HKLM\software\microsoft\windows\currentversion\bits[jobminimumretrydelay]
Queries value: HKLM\software\microsoft\windows\currentversion\bits[transferbuffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\bits[sleepatcallbackbegin]
Queries value: HKLM\software\microsoft\windows\currentversion\bits[sleepatcallbackend]
Queries value:
HKLM\software\microsoft\windows\currentversion\bits[sleepatcallbackduration]
Queries value: HKLM\software\microsoft\windows\currentversion\bits[testflags]
Queries value: HKLM\software\microsoft\windows\currentversion\bits[forcefileflush]
Queries value: HKLM\software\microsoft\windows\currentversion\bits[uselmcompat]
Queries value: HKLM\software\microsoft\windows\currentversion\bits[igdsearcherdll]
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\com3[gipactivitybypass]
Queries value: HKLM\system\currentcontrolset\services\fontcache\parameters[servicedll]
Queries value:
HKLM\system\currentcontrolset\services\fontcache\parameters[servicemanifest]
Queries value: HKLM\system\currentcontrolset\services\fontcache\parameters[servicemain]
Queries value: HKLM\system\currentcontrolset\services\ssdpsrv\parameters[servicedll]
Queries value:
HKLM\system\currentcontrolset\services\ssdpsrv\parameters[servicemanifest]
Queries value: HKLM\system\currentcontrolset\services\ssdpsrv\parameters[servicemain]
Queries value:
HKLM\system\currentcontrolset\services\fontcache\parameters[initialtimeout]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[e856c26a-e105-4683-a948-6920dcc42e45]
Queries value:
HKLM\system\currentcontrolset\services\fontcache\parameters[initialsystemcachesize]
Queries value:
HKLM\system\currentcontrolset\services\fontcache\parameters[maximumsystemcachesize]
Queries value:
HKLM\system\currentcontrolset\services\fontcache\parameters[initialusercachesize]
Queries value:
HKLM\system\currentcontrolset\services\fontcache\parameters[maximumusercachesize]
Queries value: HKLM\system\currentcontrolset\services\ssdpsrv\parameters[maxhttpsize]
Queries value:
HKLM\system\currentcontrolset\services\ssdpsrv\parameters[additionalipv6scope]
Queries value:
HKLM\system\currentcontrolset\services\ssdpsrv\parameters[includeonlylistedaddresses]
Queries value: HKLM\system\currentcontrolset\services\ssdpsrv\parameters[addresslist]
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\cryptography[machineguid]
Queries value: HKLM\system\currentcontrolset\services\ssdpsrv\parameters[ttl]
Queries value: HKLM\system\currentcontrolset\services\ssdpsrv\parameters[receivescope]
Queries value: HKLM\software\microsoft\rpc\securityservice[9]
Queries value:
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignaturedll]
Queries value:

HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignatureroutine]
Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[name]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[comment]
Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[capabilities]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[rpcid]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[version]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[type]
Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[tokensize]
Queries value: HKLM\software\microsoft\rpc\extensions[remoterpcdll]
Queries value: HKLM\system\currentcontrolset\services\ssdpsrv\parameters[maxcache]
Queries value:
HKLM\system\currentcontrolset\services\ssdpsrv\parameters[servicedllunloadonstop]
Queries value: HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}\proxystubclsid32[]
Queries value: HKCR\clsid\{00020424-0000-0000-c000-000000000046}[]
Queries value: HKCR\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32[]
Queries value: HKCR\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
Queries value: HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}\typelib[]
Queries value: HKCR\interface\{adda3d55-6f72-4319-bff9-18600a539b10}\typelib[version]
Queries value: HKCR\typelib\{db3442a7-a2e9-4a59-9cb5-f5c1a5d901e5}\1.0\0\win32[]
Queries value: HKLM\software\microsoft\rpc[udtalignmentpolicy]
Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}\proxystubclsid32[]
Queries value: HKCR\clsid\{00020420-0000-0000-c000-000000000046}[]
Queries value: HKCR\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32[]
Queries value: HKCR\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\windows\currentversion\bits[statefilechunk]
Queries value:
HKLM\software\microsoft\windows\currentversion\bits[statefilewritebuffer]
Queries value: HKLM\software\microsoft\windows\currentversion\bits[stateindex]
Queries value:
HKLM\software\microsoft\windows\currentversion\bits[gatewaysearcherdeletetime]
Queries value: HKLM\system\setup[upgradeinprogress]
Queries value: HKLM\sam\sam\domains\builtin\aliases\00000220[c]
Queries value: HKLM\sam\sam[c]
Queries value: HKLM\sam\sam\domains\builtin[v]
Queries value: HKLM\sam\sam\domains\builtin\aliases\names\administrators[]
Queries value: HKLM\sam\sam\domains\account[v]
Queries value: HKLM\sam\sam\domains\builtin\aliases\00000227[c]
Queries value: HKLM\sam\sam\domains\builtin\aliases\names\backup operators[]
Queries value:
HKLM\system\currentcontrolset\services\vss\settings[activewriterstatetimeout]
Queries value: HKLM\system\currentcontrolset\services\vss\diag[]
Queries value: HKLM\system\currentcontrolset\services\vss\settings[torncomponentsmax]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{faf53cc4-bd73-4e36-83f1-2b23f46e513e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[firinginterfaceiid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{faf53cc4-bd73-4e36-83f1-2b23f46e513e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[customconfigclsid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{faf53cc4-bd73-4e36-83f1-2b23f46e513e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[description]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{faf53cc4-bd73-4e36-83f1-2b23f46e513e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{faf53cc4-bd73-4e36-83f1-2b23f46e513e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[multiinterfacepublisherfilterclsid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{faf53cc4-bd73-4e36-83f1-2b23f46e513e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[parallelfiringtimeout]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{faf53cc4-bd73-4e36-83f1-2b23f46e513e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[allowperuserinprocactivation]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{faf53cc4-bd73-4e36-83f1-2b23f46e513e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[allowperuseractivateasactivator]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{faf53cc4-bd73-4e36-83f1-2b23f46e513e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[allowperusermoniker]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{faf53cc4-bd73-4e36-83f1-2b23f46e513e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[serialfiringtimeout]
Sets/Creates value:

HKCU\software\microsoft\windows\currentversion\run[1h6wzb8fwvux1exfmpbqaa]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[1409]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[1609]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[1406]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\1[1406]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\2[1406]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\3[1406]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\4[1406]
Sets/Creates value: HKCU\software\microsoft\internet explorer\phishingfilter[shownservicedownballoon]
Sets/Creates value: HKCU\software\microsoft\internet explorer\recovery[clearbrowsinghistoryonexit]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings[globaluseroffline]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\{1b7b6586-60aa-4cdd-91a5-554248c31a3a}[wpaddecisionreason]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\{1b7b6586-60aa-4cdd-91a5-554248c31a3a}[wpaddecisiontime]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\{1b7b6586-60aa-4cdd-91a5-554248c31a3a}[wpaddecision]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\{1b7b6586-60aa-4cdd-91a5-554248c31a3a}[wpadnetworkname]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\5e-3c-c9-eb-6a-6f[wpaddecisionreason]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\5e-3c-c9-eb-6a-6f[wpaddecisiontime]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\5e-3c-c9-eb-6a-6f[wpaddecision]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[enablehttp1_1]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[proxyhttp1.1]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[warnonpost]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[warnonpostredirect]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[warnonintranet]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[1409]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[1609]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[1406]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[1409]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[1609]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[1406]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1409]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1609]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1406]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[1409]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[1609]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[1406]
Value changes: HKCU\software\microsoft\internet explorer\phishingfilter[enabledv8]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[proxyenable]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\connections[savedlegacysettings]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\connections[defaultconnectionsettings]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\wpad[wpadlastnetwork]
Value changes: HKLM\system\currentcontrolset\services\w32time\timeproviders\ntpclient[specialpolltimeremaining]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[globaluseroffline]
Value changes: HKLM\system\currentcontrolset\services\bits\performance[perfmmfilename]

Value changes:
HKLM\system\currentcontrolset\control\backuprestore\filesnottobackup[bits_log]
Value changes:
HKLM\system\currentcontrolset\control\backuprestore\filesnottobackup[bits_bak]