Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 5011, Task ID: 40060

Task ID:	40060
Risk Level:	10
Date Processed:	2016-05-03 05:04:46 (UTC)
Processing Time:	63.3 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\spyeye_injector.exe"
Sample ID:	5011
Type:	basic
Owner:	admin
Label:	spyeye_injector.exe
Date Added:	2016-05-03 05:04:45 (UTC)
File Type:	PE32:win32:gui
File Size:	103936 bytes
MD5:	b98bb6d7428c3dbffcfcab2414c6daa2
SHA256:	fc7f54ce456c164452d8429a7fd5f52629a69338f8954e287d2664c03c37e029
Description:	None

Pattern Matching Results

5 PE: Contains compressed section
10 Creates malicious mutex: Spyeye [Banking]
2 PE: Nonstandard section
6 Modifies registry autorun entries
10 Suspicious writeprocess: Spyeye [Banking]
3 Writes to a log file [Info]
7 Writes to memory of system processes
6 Writes to system32 folder
5 Packer: UPX
1 HTTP connection - response code 404 (file not found)
5 Adds autostart object
4 Reads process memory
5 Installs service
5 Abnormal sleep detected

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\83A49421643.exe ["C:\WinOldFileq\83A49421643.exe"]
Creates process:	C:\WINDOWS\system32\wbem\wmiadap.exe [wmiadap.exe /R /T]
Reads from process:	PID:1664 C:\WINDOWS\system32\calc.exe
Reads from process:	PID:1272 C:\WINDOWS\system32\svchost.exe
Reads from process:	PID:1972 C:\WINDOWS\explorer.exe
Reads from process:	PID:1408 C:\WINDOWS\system32\wbem\wmiadap.exe
Writes to process:	PID:1972 C:\WINDOWS\explorer.exe
Writes to process:	PID:572 C:\WINDOWS\system32\winlogon.exe
Writes to process:	PID:908 C:\WINDOWS\system32\lsass.exe
Writes to process:	PID:1068 C:\WINDOWS\system32\svchost.exe
Writes to process:	PID:1148 C:\WINDOWS\system32\svchost.exe
Writes to process:	PID:1272 C:\WINDOWS\system32\svchost.exe
Writes to process:	PID:1384 C:\WINDOWS\system32\svchost.exe
Writes to process:	PID:1752 C:\WINDOWS\system32\spoolsv.exe
Writes to process:	PID:1960 C:\Program Files\Java\jre7\bin\jqs.exe
Writes to process:	PID:336 C:\Program Files\Adobe\Reader 9.0\Reader\reader_sl.exe
Writes to process:	PID:352 C:\WINDOWS\system32\ctfmon.exe
Writes to process:	PID:1240 C:\WINDOWS\system32\alg.exe
Writes to process:	PID:1456 C:\WINDOWS\system32\rundll32.exe
Writes to process:	PID:524 C:\WINDOWS\system32\wbem\unsecapp.exe
Writes to process:	PID:460 C:\WINDOWS\system32\wbem\wmiprvse.exe
Writes to process:	PID:1664 C:\WINDOWS\system32\calc.exe
Writes to process:	PID:1408 C:\WINDOWS\system32\wbem\wmiadap.exe
Terminates process:	C:\WinOldFileq\83A49421643.exe
Terminates process:	C:\WINDOWS\Temp\spyeye_injector.exe

Named Object Events

Creates mutex:	\BaseNamedObjects\RPCController
Creates mutex:	\BaseNamedObjects\zXeRY3a_PtW|00FFFFFF
Creates mutex:	\BaseNamedObjects\zXeRY3a_PtW|00000000
Creates mutex:	\BaseNamedObjects\K11777AQgSYeGW79751EQmMU97975IU
Creates mutex:	\BaseNamedObjects\c:!documents and settings!admin!local settings!temporary internet files!content.ie5!
Creates mutex:	\BaseNamedObjects\c:!documents and settings!admin!cookies!
Creates mutex:	\BaseNamedObjects\c:!documents and settings!admin!local settings!history!history.ie5!
Creates mutex:	\BaseNamedObjects\WininetConnectionMutex
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.ILH
Creates mutex:	\BaseNamedObjects\MSPMutex
Creates mutex:	\BaseNamedObjects\RAS_MO_02
Creates mutex:	\BaseNamedObjects\RAS_MO_01
Creates mutex:	\BaseNamedObjects\SHIMLIB_LOG_MUTEX
Creates mutex:	\BaseNamedObjects\ADAP_WMI_ENTRY
Creates mutex:	\BaseNamedObjects\RefreshRA_Mutex
Creates mutex:	\BaseNamedObjects\RefreshRA_Mutex_Lib
Creates mutex:	\BaseNamedObjects\RefreshRA_Mutex_Flag
Creates event:	\BaseNamedObjects\CTF.ThreadMarshalInterfaceEvent.000000C0.00000000.00000004
Creates event:	\BaseNamedObjects\CTF.ThreadMIConnectionEvent.000000C0.00000000.00000004
Creates event:	\BaseNamedObjects\MSCTF.SendReceive.Event.AM.IC

Creates event: \BaseNamedObjects\MSCTF.SendReceiveConection.Event.AM.IC
Creates event: \BaseNamedObjects\MSCTF.SendReceive.Event.ILH.IC
Creates event: \BaseNamedObjects\MSCTF.SendReceiveConection.Event.ILH.IC
Creates event: \BaseNamedObjects\crypt32LogoffEvent
Creates event: \BaseNamedObjects\DINPUTWINMM
Creates event: \BaseNamedObjects\userenv: User Profile setup event
Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore: \BaseNamedObjects\4FBEA4B1
Creates semaphore: \BaseNamedObjects\WMI_SysEvent_Semaphore_1272

File System Events

Creates: C:\WinOldFileq
Creates: C:\WinOldFileq\
Creates: C:\WinOldFileq\83A49421643.exe
Creates: C:\WinOldFileq\B20776D7F8FB639
Opens: C:\WINDOWS\Prefetch\SPYEYE_INJECTOR.EXE-255B270C.pf
Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\system32\kernel32.dll
Opens: C:\
Opens: C:\WINDOWS\system32\ntdll.dll
Opens: C:\WinOldFileq
Opens: C:\WINDOWS\system32\calc.exe
Opens: C:\WinOldFileq\
Opens: C:\WINDOWS\Temp\spyeye_injector.exe
Opens: C:\WinOldFileq\83A49421643.exe
Opens: C:\WINDOWS\AppPatch\sysmain.sdb
Opens: C:\WINDOWS\AppPatch\systest.sdb
Opens: C:\WinOldFileq\83A49421643.exe.Manifest
Opens: C:\WINDOWS\Prefetch\83A49421643.EXE-1FEF9BA6.pf
Opens: C:\WINDOWS\Temp\164d00e3-71a8-467f-a6a5-23bbe2515955
Opens: C:\WINDOWS\system32\crypt32.dll
Opens: C:\WINDOWS\system32\msasn1.dll
Opens: C:\WINDOWS\system32\imm32.dll
Opens: C:\WINDOWS\system32\ws2_32.dll
Opens: C:\WINDOWS\system32\ws2help.dll
Opens: C:\WINDOWS\system32\urlmon.dll.123.Manifest
Opens: C:\WINDOWS\system32\urlmon.dll.123.Config
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens: C:\WINDOWS\WindowsShell.Manifest
Opens: C:\WINDOWS\WindowsShell.Config
Opens: C:\WINDOWS\system32\WININET.dll.123.Manifest
Opens: C:\WINDOWS\system32\WININET.dll.123.Config
Opens: C:\WINDOWS\system32\msimg32.dll
Opens: C:\WINDOWS\system32\shell32.dll
Opens: C:\WINDOWS\system32\SHELL32.dll.124.Manifest
Opens: C:\WINDOWS\system32\SHELL32.dll.124.Config
Opens: C:\WINDOWS\system32\comctl32.dll
Opens: C:\WINDOWS\system32\comctl32.dll.124.Manifest
Opens: C:\WINDOWS\system32\comctl32.dll.124.Config
Opens: C:\WinOldFileq\B20776D7F8FB639
Opens: C:\WINDOWS\system32\user32.dll
Opens: C:\WINDOWS\system32\wininet.dll
Opens: C:\WINDOWS\system32\advapi32.dll
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5
Opens: C:\Documents and Settings\Admin\Local Settings\History
Opens: C:\Documents and Settings\Admin\Local Settings\History\History.IE5
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\index.dat
Opens: C:\Documents and Settings\Admin\Cookies
Opens: C:\Documents and Settings\Admin\Cookies\index.dat
Opens: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\index.dat
Opens: C:\WINDOWS\system32\mswsock.dll
Opens: C:\WINDOWS\system32\hnetcfg.dll
Opens: C:\WINDOWS\system32\wshtcpip.dll
Opens: C:\windows\temp\spyeye_injector.exe
Opens: C:\AUTOEXEC.BAT
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\SystemCertificates\My\Certificates
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\SystemCertificates\My\CRLs
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\SystemCertificates\My\CTLs
Opens: C:\WINDOWS\system32\MSIMTF.dll
Opens: C:\WINDOWS\system32\MSCTF.dll
Opens: C:\WINDOWS\system32\rasapi32.dll
Opens: C:\WINDOWS\system32\rasman.dll
Opens: C:\WINDOWS\system32\tapi32.dll
Opens: C:\WINDOWS\system32\TAPI32.dll.124.Manifest
Opens: C:\WINDOWS\system32\TAPI32.dll.124.Config
Opens: C:\WINDOWS\system32\tapisrv.dll
Opens: C:\Documents and Settings\All Users\Application Data\Microsoft\Network\Connections\Pbk
Opens: C:\WINDOWS\system32\ras
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Network\Connections\Pbk\
Opens: C:\WINDOWS\system32\sensapi.dll
Opens: C:\WINDOWS\system32\rasmans.dll
Opens: C:\WINDOWS\system32\winipsec.dll
Opens: C:\WINDOWS\system32\rasadhlp.dll
Opens: C:\WINDOWS\system32\dnsapi.dll
Opens: C:\WINDOWS\system32\wbem\Logs\wbemess.log
Opens: C:\WINDOWS\system32\winrnr.dll
Opens: C:\WINDOWS\system32\sens.dll
Opens: C:\WINDOWS\system32\mprapi.dll

Opens: C:\WINDOWS\system32\activeds.dll
Opens: C:\WINDOWS\system32\adsldpc.dll
Opens: C:\WINDOWS\system32\samlib.dll
Opens: C:\WINDOWS\system32\rastapi.dll
Opens: C:\WINDOWS\system32\unimdm.tsp
Opens: C:\WINDOWS\system32\uniplat.dll
Opens: C:\WINDOWS\system32\kmddsp.tsp
Opens: C:\WINDOWS\system32\ndptsp.tsp
Opens: C:\WINDOWS\system32\ipconf.tsp
Opens: C:\WINDOWS\system32\h323.tsp
Opens: C:\WINDOWS\system32\h323log.txt
Opens: C:\WINDOWS\system32\hidphone.tsp
Opens: C:\WINDOWS\system32\hid.dll
Opens: C:\WINDOWS\system32\rasppp.dll
Opens: C:\WINDOWS\system32\ntlsapi.dll
Opens: C:\WINDOWS\system32\kerberos.dll
Opens: C:\WINDOWS\system32\cryptdll.dll
Opens: C:\WINDOWS\win.ini
Opens: C:\WINDOWS\system32\rasqec.dll
Opens: C:\WINDOWS\system32\msv1_0.dll
Opens: C:\WINDOWS\system32\drprov.dll
Opens: C:\WINDOWS\system32\ntlanman.dll
Opens: C:\WINDOWS\system32\netui0.dll
Opens: C:\WINDOWS\system32\netui1.dll
Opens: C:\WINDOWS\system32\netrap.dll
Opens: C:\WINDOWS\system32\davclnt.dll
Opens: C:\WINDOWS\system32\wbem\Repository\$WinMgmt.CFG
Opens: C:\WINDOWS\system32\wbem\wmiadap.exe
Opens: C:\WINDOWS\system32\apphelp.dll
Opens: C:\WINDOWS\system32\wbem
Opens: C:\WINDOWS
Opens: C:\WINDOWS\system32
Opens: C:\WINDOWS\system32\WBEM\WMIADAP.EXE.Manifest
Opens: C:\WINDOWS\Prefetch\WMIADAP.EXE-2DF425B2.pf
Opens: C:
Opens: C:\WINDOWS\AppPatch
Opens: C:\WINDOWS\Registration
Opens: C:\WINDOWS\system32\config
Opens: C:\WINDOWS\system32\wbem\Repository
Opens: C:\WINDOWS\system32\wbem\Repository\FS
Opens: C:\WINDOWS\WinSxS
Opens: C:\WINDOWS\system32\unicode.nls
Opens: C:\WINDOWS\system32\locale.nls
Opens: C:\WINDOWS\system32\sorttbls.nls
Opens: C:\WINDOWS\system32\msvcrt.dll
Opens: C:\WINDOWS\system32\msvcp60.dll
Opens: C:\WINDOWS\system32\rpcrt4.dll
Opens: C:\WINDOWS\system32\secur32.dll
Opens: C:\WINDOWS\system32\wbem\wbemcomn.dll
Opens: C:\WINDOWS\system32\ole32.dll
Opens: C:\WINDOWS\system32\gdi32.dll
Opens: C:\WINDOWS\system32\oleaut32.dll
Opens: C:\WINDOWS\system32\loadperf.dll
Opens: C:\WINDOWS\system32\shimeng.dll
Opens: C:\WINDOWS\AppPatch\AcGenral.dll
Opens: C:\WINDOWS\system32\winmm.dll
Opens: C:\WINDOWS\system32\msacm32.dll
Opens: C:\WINDOWS\system32\version.dll
Opens: C:\WINDOWS\system32\shlwapi.dll
Opens: C:\WINDOWS\system32\userenv.dll
Opens: C:\WINDOWS\system32\uxtheme.dll
Opens: C:\WINDOWS\system32\ctype.nls
Opens: C:\WINDOWS\system32\sortkey.nls
Opens: C:\WINDOWS\system32\rpcss.dll
Opens: C:\WINDOWS\system32\winlogon.exe
Opens: C:\WINDOWS\system32\xpsp2res.dll
Opens: C:\WINDOWS\system32\psapi.dll
Opens: C:\WINDOWS\system32\ntmarta.dll
Opens: C:\WINDOWS\system32\wldap32.dll
Opens: C:\WINDOWS\system32\clbcatq.dll
Opens: C:\WINDOWS\system32\comres.dll
Opens: C:\WINDOWS\Registration\R000000000007.clb
Opens: C:\WINDOWS\system32\wbem\wbemprox.dll
Opens: C:\WINDOWS\system32\wbem\wbemsvc.dll
Opens: C:\WINDOWS\system32\wbem\fastprox.dll
Opens: C:\WINDOWS\system32\ntdsapi.dll
Opens: C:\WINDOWS\system32\netapi32.dll
Opens: C:\WINDOWS\system32\wbem\Repository\FS\OBJECTS.DATA
Opens: C:\WINDOWS\SYSTEM32\WBEM\PERFORMANCE\WMIAPRPL_NEW.H
Opens: C:\WINDOWS\SYSTEM32\WBEM\PERFORMANCE\WMIAPRPL_NEW.INI
Opens: C:\WINDOWS\system32\perfc009.dat
Opens: C:\WINDOWS\system32\perfh009.dat
Opens: C:\WINDOWS\SYSTEM32\CONFIG\SYSTEM
Opens: C:\WINDOWS\SYSTEM32\PERFSTRINGBACKUP.TMP
Opens: C:\WINDOWS\system32\PerfStringBackup.INI
Opens: C:\WINDOWS\TEMP\PERFLIB_PERFDATA_E6C.DAT
Opens: C:\WINDOWS\system32\wbem\Repository\FS\INDEX.BTR
Opens: C:\WINDOWS\TEMP\PERFLIB_PERFDATA_570.DAT
Opens: C:\WINDOWS\system32\wbem\Logs\wbemcore.log
Opens: C:\WINDOWS\system32\wbem\wmiprov.dll
Opens: C:\WINDOWS\system32\wmi.dll
Opens: C:\WINDOWS\system32\wbem\Logs\wmiprov.log
Opens: C:0409\
Opens: C:\WINDOWS\MUI\Fallback\0409\
Opens: C:\WINDOWS\system32\DRIVERS\MUI\0409\
Opens: C:\WINDOWS\System32\Drivers\MUI\0409\
Opens: C:\WINDOWS\system32\wbem\mofd.dll
Opens: C:\WINDOWS\system32\drivers\acpi.sys
Writes to: C:\WinOldFileq\83A49421643.exe
Writes to: C:\WinOldFileq\B20776D7F8FB639
Writes to: C:\WINDOWS\system32\wbem\Logs\wbemess.log

Writes to:	C:\WINDOWS\system32\wbem\Logs\wbemcore.log
Writes to:	C:\WINDOWS\system32\wbem\Logs\wmiprov.log
Reads from:	C:\WINDOWS\system32\ntdll.dll
Reads from:	C:\WINDOWS\system32\calc.exe
Reads from:	C:\WINDOWS\Temp\spyeye_injector.exe
Reads from:	C:\WinOldFileq\B20776D7F8FB639
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:\WinOldFileq\83A49421643.exe
Reads from:	C:\WINDOWS\system32\crypt32.dll
Reads from:	C:\AUTOEXEC.BAT
Reads from:	C:\WINDOWS\system32\sens.dll
Reads from:	C:\WINDOWS\win.ini
Reads from:	C:\WINDOWS\system32\wbem\Repository\$WinMgmt.CFG
Reads from:	C:\WINDOWS\Prefetch\WMIADAP.EXE-2DF425B2.pf
Reads from:	C:\WINDOWS\Registration\R000000000007.clb
Deletes:	C:\WINDOWS\Temp\spyeye_injector.exe

Network Events

DNS query:	alexeyartemov.com
DNS response:	alexeyartemov.com ⇒ 198.105.244.11
DNS response:	alexeyartemov.com ⇒ 104.239.213.7
Connects to:	88.198.13.147:443
Connects to:	198.105.244.11:80
Connects to:	104.239.213.7:80
Sends data to:	8.8.8.8:53
Sends data to:	88.198.13.147:443
Sends data to:	4.2.2.1:53
Sends data to:	alexeyartemov.com:80 (198.105.244.11)
Sends data to:	alexeyartemov.com:80 (104.239.213.7)
Receives data from:	4.2.2.1:53
Receives data from:	alexeyartemov.com:80 (198.105.244.11)
Receives data from:	8.8.8.8:53
Receives data from:	alexeyartemov.com:80 (104.239.213.7)

Windows Registry Events

Creates key:	HKCU\sessioninformation
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings
Creates key:	HKCU\software\microsoft\windows\currentversion\run
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:	HKLM\software\classes
Creates key:	HKU\.default\software\microsoft\windows\currentversion\internet settings
Creates key:	HKCU\software\microsoft\windows\currentversion\explorer\user shell folders
Creates key:	HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Creates key:	HKCU\software\microsoft\systemcertificates\my
Creates key:	HKCU\software\microsoft\windows nt\currentversion\winlogon
Creates key:	HKCU\software\microsoft windows
Creates key:	HKLM\software\microsoft\windows\currentversion\explorer\user shell folders
Creates key:	HKLM\software\microsoft\windows\currentversion\explorer\shell folders
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings\connections
Creates key:	HKCU\software\microsoft\windows nt\currentversion\network\location awareness
Creates key:	HKLM\system\currentcontrolset\services\tcpip\parameters
Creates key:	HKLM\system\currentcontrolset\services\netbt\parameters
Creates key:	HKU\.default\software\microsoft\windows\currentversion\telephony\handoffpriorities\mediamodes
Creates key:	HKLM\software\microsoft\windows\currentversion\h323tsp
Creates key:	HKLM\system\currentcontrolset\services\eventlog\application\microsoft h.323 telephony service provider
Creates key:	HKLM\system\currentcontrolset\control\deviceclasses
Creates key:	HKLM\software\microsoft\wbem\cimom
Creates key:	HKU\.default\software\microsoft\multimedia\audio
Creates key:	HKU\.default\software\microsoft\multimedia\audio compression manager\
Creates key:	HKU\.default\software\microsoft\multimedia\audio compression manager\msacm
Creates key:	HKU\.default\software\microsoft\multimedia\audio compression manager\priority v4.00
Creates key:	HKLM\software\microsoft\wbem\wdm
Creates key:	HKLM\system\currentcontrolset\services\sharedaccess\epoch
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]
Deletes value:	HKLM\software\microsoft\wbem\wdm[wmibinarymofresource.highdatetime=29924836,lowdatetime=41836544,name="c:\\windows\\system32\\advapi32.dll[mofresourcename]"]
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\spyeye_injector.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\secur32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rpcrt4.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\advapi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\winlogon
Opens key: HKLM\
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntdll.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\system\currentcontrolset\control\computername
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKCU\software\classes\applications\calc.exe
Opens key: HKCR\applications\calc.exe
Opens key: HKCU\software\microsoft\windows\shellnoroam\muicache\
Opens key: HKLM\system\wpa\tabletpc
Opens key: HKLM\system\wpa\mediacenter
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\83a49421643.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\83a49421643.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\gdi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\user32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\imm32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msasn1.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\crypt32.dll
Opens key: HKLM\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\system\currentcontrolset\services\crypt32\performance
Opens key: HKLM\software\microsoft\windows nt\currentversion\msasn1
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ws2help.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ws2_32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shlwapi.dll
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\normaliz.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ole32.dll
Opens key: HKLM\software\microsoft\ole
Opens key: HKCR\interface
Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\oleaut32.dll
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\fileassociation
Opens key: HKLM\software\microsoft\oleaut
Opens key: HKLM\software\microsoft\oleaut\userera
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\iertutil.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\urlmon.dll
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comctl32.dll
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wininet.dll
Opens key: HKCU\software\classes\
Opens key: HKCU\software\classes\protocols\name-space handler\
Opens key: HKCR\protocols\name-space handler
Opens key: HKCU\software\classes\protocols\name-space handler
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\
Opens key: HKLM\software\microsoft\ctf\tip\
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-

c9633f71be64}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
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_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
Opens key: HKLM\system\currentcontrolset\control\wmi\security
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msimg32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shell32.dll
Opens key: HKLM\system\setup
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\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: 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\software\policies\microsoft\internet explorer\main
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
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: HKU\.default\software\policies\microsoft\control panel\desktop
Opens key: HKU\.default\control panel\desktop
Opens key: HKCR\protocols\name-space handler\
Opens key: HKU\.default\software\policies\microsoft\windows\currentversion\internet
settings
Opens key: HKU\.default\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
Opens key: HKU\.default\software\policies\microsoft\internet
explorer\main\featurecontrol
Opens key: HKU\.default\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKU\.default\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key: HKU\.default\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\

Opens key: HKU\.default\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
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\000000000003
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache\content
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
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\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: 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\protocol_catalog9\catalog_entries\000000000009
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key: HKLM\security\policy
Opens key: HKLM\security\policy\secdesc
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
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: 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: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat
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\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\mshist012014033120140407
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mswsock.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\hnetcfg.dll
Opens key: HKLM\software\microsoft\rpc\securityservice
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012014041220140413
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\privacie:
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wshtcpip.dll
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_use_spn_for_ntlm_auth_disabled
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
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_passport_check_302_for_success_kb949059
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
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: HKLM\sam\sam\domains\account\groups\000003eb
Opens key: HKLM\sam\sam\domains\account\aliases\000003eb
Opens key: HKLM\sam\sam\domains\account\users\000003eb
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\systemcertificates\my\physicalstores
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist
Opens key: HKLM\system\currentcontrolset\control\session manager\environment
Opens key: HKLM\software\microsoft\windows\currentversion
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003
Opens key: HKCU\environment
Opens key: HKCU\volatile environment
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\systemcertificates\my\crls
Opens key: HKCU\software\microsoft\systemcertificates\my\ctls
Opens key: HKCU\software\microsoft\systemcertificates\my\keys
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasman.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\tapi32.dll
Opens key: HKLM\software\microsoft\windows\currentversion\telephony
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasapi32.dll
Opens key: HKLM\software\microsoft\tracing\rasapi32
Opens key: HKLM\system\currentcontrolset\services
Opens key: HKLM\system\currentcontrolset\services\tapisrv
Opens key: HKLM\system\currentcontrolset\services\tapisrv\parameters
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\tapisrv.dll
Opens key: HKLM\software\microsoft\tracing\tapisrv
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\sensapi.dll
Opens key: HKLM\software\microsoft\com3
Opens key: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}
Opens key: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\treatas
Opens key: HKCR\
Opens key: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprocserver32
Opens key: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprocserverx86
Opens key: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\localserver32
Opens key: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprochandler32
Opens key: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprochandlerx86
Opens key: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\localserver
Opens key: HKCR\appid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\http filters\rpa
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\http filters\rpa
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\system\currentcontrolset\control\productoptions
Opens key: HKLM\software\policies\microsoft\system\dnsclient
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key: HKLM\software\microsoft\windows\currentversion\telephony\server
Opens key: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}
Opens key: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\treatas
Opens key: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprocserver32
Opens key: HKLM\system\currentcontrolset\services\rasman
Opens key: HKLM\system\currentcontrolset\services\rasman\parameters
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winipsec.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasmans.dll
Opens key: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprocserverx86
Opens key: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\localserver32
Opens key: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprochandler32
Opens key: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprochandlerx86
Opens key: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasadhlp.dll
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
Opens key: HKLM\software\policies\microsoft\internet explorer\security
Opens key: HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}
Opens key: HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\treatas
Opens key: HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\inprocserver32
Opens key: HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\inprocserverx86
Opens key: HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\localserver32
Opens key: HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\inprochandler32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dnsapi.dll
Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient
Opens key: HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\inprochandlerx86
Opens key: HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\localserver
Opens key: HKLM\system\currentcontrolset\control\network
Opens key: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}
Opens key: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi
Opens key: HKU\.default\software\microsoft\windows\shellnoroam\muicache\
Opens key: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi\interfaces
Opens key: HKU\s-1-5-18_classes
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}
Opens key: HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}
Opens key: HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\treatas
Opens key: HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\inprocserver32
Opens key: HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\inprocserverx86
Opens key: HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\localserver32
Opens key: HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}
Opens key: HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\treatas
Opens key: HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\inprocserver32
Opens key: HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\inprochandler32
Opens key: HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\inprochandlerx86
Opens key: HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\localserver
Opens key: HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\inprocserverx86
Opens key: HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\localserver32
Opens key: HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\inprochandler32
Opens key: HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\inprochandlerx86
Opens key: HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\localserver
Opens key: HKLM\system\currentcontrolset\services\eventlog\system
Opens key: HKLM\system\currentcontrolset\services\eventlog\system\service control
manager
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\ndi
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\ndi\interfaces
Opens key: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\ndi
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\ndi\interfaces
Opens key: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\treatas
Opens key: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprocserver32
Opens key: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprocserverx86
Opens key: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\localserver32
Opens key: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprochandler32
Opens key: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprochandlerx86
Opens key: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\localserver
Opens key: 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}
Opens key: HKLM\system\currentcontrolset\services\tcpip
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\adapters
Opens key:

HKLM\system\currentcontrolset\services\tcpip\parameters\adapters\ndiswanip
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\winrnr.dll
Opens key: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}\typelib
Opens key: HKCR\typelib
Opens key: HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}
Opens key: HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}\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: HKLM\system\currentcontrolset\services\dhcp\configurations\alternate_{16325b0b-4636-4303-abe3-c7d49d7cecdc}
Opens key: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}
Opens key: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}
Opens key: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{d789ab02-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}
Opens key: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi
Opens key: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi\interfaces
Opens key: HKLM\system\currentcontrolset\services\vxd\mstcp
Opens key: HKLM\system\currentcontrolset\control\computername\computername
Opens key: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\adsldpc.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\activeds.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\samlib.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mprapi.dll
Opens key: HKLM\system\currentcontrolset\services\netbt
Opens key: HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
Opens key: HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{16325b0b-4636-4303-abe3-c7d49d7cecdc}
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rastapi.dll
Opens key: HKLM\software\microsoft\tracing\rastapi
Opens key: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{1ec466dd-2b44-4231-a775-cbd69f6eb46b}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}
Opens key: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{4d99c768-0774-4b40-ac15-8342c658aad1}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}
Opens key: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{68b25be9-46e1-45c1-8062-41b3d17a79a0}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}
Opens key: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{6b9c1fb5-c711-47f3-94f9-bac5ad5535fe}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}
Opens key: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{7f7b0a42-f639-4f28-9cf7-9338fedc54f0}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}
Opens key: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{913b976b-c04f-4957-90ef-c1ee4d66edfc}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}
Opens key: HKLM\software\microsoft\tracing\tapi32
Opens key: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{a637889b-9e0a-4dc0-8316-d42b20771b16}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}
Opens key: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{b8808a2b-4188-47e6-85ae-d3e76088cdae}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}
Opens key: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}\publisherproperties
Opens key: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}\subscriberproperties
Opens key: HKU\.default\software\microsoft\windows\currentversion\telephony\handoffpriorities
Opens key: HKLM\software\microsoft\windows\currentversion\telephony\providers
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\uniplat.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\unimdm.tsp
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\kmddsp.tsp
Opens key: HKLM\software\microsoft\tracing\kmddsp
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ndptsp.tsp
Opens key: HKLM\software\microsoft\tracing\ndptsp
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ipconf.tsp
Opens key: HKLM\software\microsoft\tracing\conftsp
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\h323.tsp
Opens key: HKLM\system\currentcontrolset\services\eventlog\application
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\hid.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\hidphone.tsp
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-001111000030}
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318}
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0002
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0003
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006
Opens key: HKLM\system\currentcontrolset\services\remoteaccess
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007
Opens key: HKLM\system\currentcontrolset\services\nbf\linkage
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntlsapi.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasppp.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\cryptdll.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\kerberos.dll
Opens key: HKLM\system\currentcontrolset\services\rasman\parameters\quarantine
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasqec.dll
Opens key: HKLM\software\microsoft\tracing\rasqec
Opens key: HKLM\software\microsoft\tracing\rasman
Opens key: HKLM\software\microsoft\tracing\ppp
Opens key: HKLM\software\microsoft\tracing\bap
Opens key: HKLM\system\currentcontrolset\services\rasman\ppp
Opens key: HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols
Opens key: HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin
Opens key: HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\chap
Opens key: HKLM\software\microsoft\tracing\rasspap
Opens key: HKLM\system\currentcontrolset\services\rasman\ppp\spap
Opens key: HKLM\software\microsoft\tracing\raspap
Opens key: HKLM\software\microsoft\tracing\raseap
Opens key: HKLM\system\currentcontrolset\services\rasman\ppp\eap
Opens key: HKLM\system\currentcontrolset\services\rasman\ppp\eap\13
Opens key: HKLM\system\currentcontrolset\services\rasman\ppp\eap\25
Opens key: HKLM\system\currentcontrolset\services\rasman\ppp\eap\26
Opens key: HKLM\system\currentcontrolset\services\rasman\ppp\eap\4
Opens key: HKLM\software\microsoft\tracing\rasccp
Opens key: HKLM\software\microsoft\tracing\rasbacp
Opens key: HKLM\software\microsoft\tracing\rasiphlp
Opens key: HKLM\system\currentcontrolset\control\securityproviders
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll
Opens key: HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msv1_0.dll
Opens key: HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4fe87b73-b12e-47d6-82c4-fb0d4cf73262}
Opens key: HKLM\system\currentcontrolset\services\netbt\parameters
Opens key: HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{4fe87b73-b12e-47d6-82c4-fb0d4cf73262}
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{cac79791-bd6d-4f3e-bcad-e3686652faee}
Opens key: HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{cac79791-bd6d-4f3e-bcad-e3686652faee}
Opens key: HKLM\software\microsoft\tracing\rasipcp
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mpr.dll
Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder
Opens key: HKLM\system\currentcontrolset
Opens key: HKLM\system\currentcontrolset\services\rdpnp\networkprovider
Opens key: HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider
Opens key: HKLM\system\currentcontrolset\services\webclient\networkprovider
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\drprov.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\netui0.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\network\world full access shared parameters
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\netrap.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\netui1.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntlanman.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\davclnt.dll
Opens key: HKCU\network
Opens key: HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}
Opens key: HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\treatas
Opens key: HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\inprocserver32
Opens key: HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\inprocserverx86
Opens key: HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\localserver32
Opens key: HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\inprochandler32
Opens key: HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\inprochandlerx86

Opens key: HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\localserver
Opens key: HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}
Opens key: HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\treatas
Opens key: HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\inprocserver32
Opens key: HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\inprocserverx86
Opens key: HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\localserver32
Opens key: HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\inprochandler32
Opens key: HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\inprochandlerx86
Opens key: HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\localserver
Opens key: HKLM\system\currentcontrolset\control\minint
Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\apphelp.dll
Opens key: HKU\.default\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\wmiadap.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKU\.default\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wmiadap.exe
Opens key: HKCU\appevents\schemes\apps\.default\systemnotification\.current
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\acgenral.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcp60.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wbemcomn.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\loadperf.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shimeng.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\winmm.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msacm32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\version.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\userenv.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\uxtheme.dll
Opens key: HKU\.default\control panel\international
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\microsoft\rpc\pagedbuffers
Opens key: HKLM\software\microsoft\rpc
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wmiadap.exe\rpcthreadpoolthrottle
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\microsoft\windows nt\currentversion\drivers32
Opens key: HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm
Opens key: HKLM\system\currentcontrolset\control\mediaresources\acm
Opens key: HKU\.default\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKU\.default\software\microsoft\windows\currentversion\explorer\user shell folders
Opens key: HKLM\software\policies\microsoft\windows\system
Opens key: HKU\.default\software\microsoft\windows\currentversion\thememanager
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key: HKLM\software\microsoft\wbem\cimom
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\psapi.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\xpsp2res.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wldap32.dll
Opens key: HKLM\system\currentcontrolset\services\ldap
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntmarta.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comres.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\clbcatq.dll
Opens key: HKLM\software\microsoft\com3\debug
Opens key: HKLM\software\classes
Opens key: HKU\
Opens key: HKCR\clsid
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\treatas
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserverx86

Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\localserver32
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler32
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandlerx86
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wbemprox.dll
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\treatas
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserver32
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserverx86
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver32
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandler32
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandlerx86
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver
Opens key: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\treatas
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserverx86
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\localserver32
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler32
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandlerx86
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\localserver
Opens key: HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}
Opens key: HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wbemsvc.dll
Opens key: HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}
Opens key: HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\treatas
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserverx86
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\localserver32
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandler32
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandlerx86
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\localserver
Opens key: HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}
Opens key: HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\netapi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntdsapi.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\fastprox.dll
Opens key: HKCR\clsid\{cd1abfc8-6c5e-4a8d-b90b-2a3b153b886d}
Opens key: HKCR\clsid\{cd1abfc8-6c5e-4a8d-b90b-2a3b153b886d}\treatas
Opens key: HKCR\clsid\{cd1abfc8-6c5e-4a8d-b90b-2a3b153b886d}\inprocserver32
Opens key: HKCR\clsid\{cd1abfc8-6c5e-4a8d-b90b-2a3b153b886d}\inprocserverx86
Opens key: HKCR\clsid\{cd1abfc8-6c5e-4a8d-b90b-2a3b153b886d}\localserver32
Opens key: HKCR\clsid\{cd1abfc8-6c5e-4a8d-b90b-2a3b153b886d}\inprochandler32
Opens key: HKCR\clsid\{cd1abfc8-6c5e-4a8d-b90b-2a3b153b886d}\inprochandlerx86
Opens key: HKCR\clsid\{cd1abfc8-6c5e-4a8d-b90b-2a3b153b886d}\localserver
Opens key: HKCR\clsid\{9a653086-174f-11d2-b5f9-00104b703efd}
Opens key: HKCR\clsid\{9a653086-174f-11d2-b5f9-00104b703efd}\treatas
Opens key: HKCR\clsid\{9a653086-174f-11d2-b5f9-00104b703efd}\inprocserver32
Opens key: HKCR\clsid\{9a653086-174f-11d2-b5f9-00104b703efd}\inprocserverx86
Opens key: HKCR\clsid\{9a653086-174f-11d2-b5f9-00104b703efd}\localserver32
Opens key: HKCR\clsid\{9a653086-174f-11d2-b5f9-00104b703efd}\inprochandler32
Opens key: HKCR\clsid\{9a653086-174f-11d2-b5f9-00104b703efd}\inprochandlerx86
Opens key: HKCR\clsid\{9a653086-174f-11d2-b5f9-00104b703efd}\localserver
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\treatas
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserverx86
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\localserver32
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler32
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandlerx86
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\localserver
Opens key: HKCR\interface\{027947e1-d731-11ce-a357-000000000001}
Opens key: HKCR\interface\{027947e1-d731-11ce-a357-000000000001}\proxystubclsid32
Opens key: HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}
Opens key: HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}\proxystubclsid32
Opens key: HKCR\clsid\{cc9072ab-c000-49d8-a5aa-00266c8dbb9b}
Opens key: HKCR\clsid\{cc9072ab-c000-49d8-a5aa-00266c8dbb9b}\treatas
Opens key: HKCR\clsid\{cc9072ab-c000-49d8-a5aa-00266c8dbb9b}\inprocserver32
Opens key: HKCR\clsid\{cc9072ab-c000-49d8-a5aa-00266c8dbb9b}\inprocserverx86
Opens key: HKCR\clsid\{cc9072ab-c000-49d8-a5aa-00266c8dbb9b}\localserver32
Opens key: HKCR\clsid\{cc9072ab-c000-49d8-a5aa-00266c8dbb9b}\inprochandler32
Opens key: HKCR\clsid\{cc9072ab-c000-49d8-a5aa-00266c8dbb9b}\inprochandlerx86
Opens key: HKCR\clsid\{cc9072ab-c000-49d8-a5aa-00266c8dbb9b}\localserver
Opens key: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}
Opens key: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32
Opens key: HKCR\clsid\{d2d588b5-d081-11d0-99e0-00c04fc2f8ec}
Opens key: HKCR\clsid\{d2d588b5-d081-11d0-99e0-00c04fc2f8ec}\inprocserver32
Opens key: HKCR\clsid\{d2d588b5-d081-11d0-99e0-00c04fc2f8ec}\localserver32
Opens key: HKCR\clsid\{eac8a024-21e2-4523-ad73-a71a0aa2f56a}
Opens key: HKCR\clsid\{eac8a024-21e2-4523-ad73-a71a0aa2f56a}\treatas
Opens key: HKCR\clsid\{eac8a024-21e2-4523-ad73-a71a0aa2f56a}\inprocserver32
Opens key: HKCR\clsid\{eac8a024-21e2-4523-ad73-a71a0aa2f56a}\inprocserverx86
Opens key: HKCR\clsid\{eac8a024-21e2-4523-ad73-a71a0aa2f56a}\localserver32
Opens key: HKCR\clsid\{eac8a024-21e2-4523-ad73-a71a0aa2f56a}\inprochandler32
Opens key: HKCR\clsid\{eac8a024-21e2-4523-ad73-a71a0aa2f56a}\inprochandlerx86
Opens key: HKCR\clsid\{eac8a024-21e2-4523-ad73-a71a0aa2f56a}\localserver
Opens key: HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}
Opens key: HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\treatas
Opens key: HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprocserver32
Opens key: HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprocserverx86
Opens key: HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\localserver32
Opens key: HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprochandler32
Opens key: HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprochandlerx86

Opens key: HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\localserver
Opens key: HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\implemented
categories\{00000003-0000-0000-c000-000000000046}
Opens key: HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}
Opens key: HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\treatas
Opens key: HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\inprocserver32
Opens key: HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\inprocserverx86
Opens key: HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\localserver32
Opens key: HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\inprochandler32
Opens key: HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\inprochandlerx86
Opens key: HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\localserver
Opens key: HKCR\clsid\{d2d588b5-d081-11d0-99e0-00c04fc2f8ec}\treatas
Opens key: HKCR\clsid\{d2d588b5-d081-11d0-99e0-00c04fc2f8ec}\inprocserverx86
Opens key: HKCR\clsid\{d2d588b5-d081-11d0-99e0-00c04fc2f8ec}\inprochandler32
Opens key: HKCR\clsid\{d2d588b5-d081-11d0-99e0-00c04fc2f8ec}\inprochandlerx86
Opens key: HKCR\clsid\{d2d588b5-d081-11d0-99e0-00c04fc2f8ec}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wmiprov.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wmi.dll
Opens key: HKLM\software\microsoft\wbem\wdm
Opens key: HKLM\system\currentcontrolset\control\nls\muilanguages
Opens key: HKLM\system\currentcontrolset\services\acpi
Opens key: HKLM\system\currentcontrolset\services\mssmbios
Opens key: HKLM\system\currentcontrolset\services\pcnet
Opens key: HKLM\system\currentcontrolset\services\ipnat
Opens key: HKLM\system\currentcontrolset\services\http
Opens key: HKCR\clsid\{c10b4771-4da0-11d2-a2f5-00c04f86fb7d}
Opens key: HKCR\clsid\{c10b4771-4da0-11d2-a2f5-00c04f86fb7d}\treatas
Opens key: HKCR\clsid\{c10b4771-4da0-11d2-a2f5-00c04f86fb7d}\inprocserver32
Opens key: HKCR\clsid\{c10b4771-4da0-11d2-a2f5-00c04f86fb7d}\inprocserverx86
Opens key: HKCR\clsid\{c10b4771-4da0-11d2-a2f5-00c04f86fb7d}\localserver32
Opens key: HKCR\clsid\{c10b4771-4da0-11d2-a2f5-00c04f86fb7d}\inprochandler32
Opens key: HKCR\clsid\{c10b4771-4da0-11d2-a2f5-00c04f86fb7d}\inprochandlerx86
Opens key: HKCR\clsid\{c10b4771-4da0-11d2-a2f5-00c04f86fb7d}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mofd.dll
Opens key: HKCR\clsid\{cb8555cc-9128-11d1-ad9b-00c04fd8fdff}
Opens key: HKCR\clsid\{cb8555cc-9128-11d1-ad9b-00c04fd8fdff}\treatas
Opens key: HKCR\clsid\{cb8555cc-9128-11d1-ad9b-00c04fd8fdff}\inprocserver32
Opens key: HKCR\clsid\{cb8555cc-9128-11d1-ad9b-00c04fd8fdff}\inprocserverx86
Opens key: HKCR\clsid\{cb8555cc-9128-11d1-ad9b-00c04fd8fdff}\localserver32
Opens key: HKCR\clsid\{cb8555cc-9128-11d1-ad9b-00c04fd8fdff}\inprochandler32
Opens key: HKCR\clsid\{cb8555cc-9128-11d1-ad9b-00c04fd8fdff}\inprochandlerx86
Opens key: HKCR\clsid\{cb8555cc-9128-11d1-ad9b-00c04fd8fdff}\localserver
Opens key: HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\implemented
categories\{00000003-0000-0000-c000-000000000046}
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKCU\control panel\desktop[multiuilanguageid]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value:
HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\calc.exe]
Queries value: HKLM\system\wpa\mediacenter[installed]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[83a49421643]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[83a49421643]
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
Queries value: HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
Queries value: HKLM\software\microsoft\ole[rwlockresourcetimeout]
Queries value: HKCR\interface[interfacehelperdisableall]
Queries value: HKCR\interface[interfacehelperdisableallforole32]
Queries value: HKCR\interface[interfacehelperdisabletypelib]
Queries value: HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableall]
Queries value: HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableallforole32]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\fileassociation[cutlist]
Queries value: HKCU\control panel\desktop[smoothscroll]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[83a49421643.exe]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}[dword]
Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}[dword]
Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}[dword]
Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[dword]
Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}[dword]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
ab78-1084642581fb]

Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}[dword]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-0000-000000000000]
Queries value: HKLM\system\setup[systemsetupinprogress]
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\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[fromcachetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[secureprotocols]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[security_hklm_only]
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: HKCU\software\microsoft\windows\currentversion\internet settings[enablehttp1_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: HKCU\software\microsoft\internet explorer\main\featurecontrol[feature_clientauthcertfilter]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol[feature_clientauthcertfilter]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[clientauthbuiltinui]
Queries value: HKU\.default\control panel\desktop[multiuilanguageid]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[lsass.exe]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[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\000000000002[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[peruseritem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[calc.exe]
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: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[cacheprefix]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]

Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cachelimit]
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: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
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: 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\security\policy\secdesc[]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
Queries value: 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:
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\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: 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:
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\000000000003[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
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:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]

Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
Queries value: 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\mshist012014033120140407[cacherepair]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
Queries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
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: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
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\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\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[disablent4rascheck]
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[bypassftptimecheck]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[releasesocketduringauth]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[releasesocketduring401auth]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[releasesocketduring401auth]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[wpadsearchalldomains]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablelegacypreauthasserver]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[disablelegacypreauthasserver]
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[warnonbadcertsending]
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: HKCU\software\microsoft\windows\currentversion\internet settings[globaluseroffline]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[enableautodial]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[urlencoding]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[truncatefilename]
Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[badproxyexpirestime]
Queries value: HKLM\sam\sam\domains\account\users\000003eb[v]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[appdata]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[profilesdirectory]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[allusersprofile]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[defaultuserprofile]
Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir]
Queries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003[profileimagepath]
Queries value: HKCU\software\microsoft\windows nt\currentversion\winlogon[parseautoexec]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[reader_sl.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[winlogon.exe]
Queries value: HKLM\software\microsoft\windows\currentversion\telephony[tapi32maxnumrequestretries]
Queries value: HKLM\software\microsoft\windows\currentversion\telephony[tapi32requestretrytimeout]
Queries value: HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\rasapi32[filedirectory]
Queries value: HKLM\software\microsoft\tracing\netshell[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\netshell[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\netshell[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\netshell[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\netshell[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\netshell[filedirectory]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[common appdata]
Queries value: HKLM\system\currentcontrolset\services\tapisrv\parameters[servicedll]
Queries value: HKLM\system\currentcontrolset\services\tapisrv\parameters[servicemain]
Queries value: HKLM\software\microsoft\tracing\tapisrv[enabledebuggertracing]
Queries value: HKLM\software\microsoft\tracing\tapisrv[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\tapisrv[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\tapisrv[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\tapisrv[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\tapisrv[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\tapisrv[filedirectory]
Queries value: HKLM\software\microsoft\tracing\wzctrace[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\wzctrace[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\wzctrace[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\wzctrace[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\wzctrace[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\wzctrace[filedirectory]
Queries value: HKLM\software\microsoft\tracing\eapol[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\eapol[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\eapol[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\eapol[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\eapol[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\eapol[filedirectory]
Queries value: HKLM\software\microsoft\tracing\eapolqec[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\eapolqec[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\eapolqec[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\eapolqec[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\eapolqec[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\eapolqec[filedirectory]
Queries value: HKLM\software\microsoft\tracing\eapolqeccb[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\eapolqeccb[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\eapolqeccb[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\eapolqeccb[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\eapolqeccb[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\eapolqeccb[filedirectory]
Queries value: HKLM\software\microsoft\tracing\svchost_rastls[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\svchost_rastls[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\svchost_rastls[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\svchost_rastls[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\svchost_rastls[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\svchost_rastls[filedirectory]
Queries value: HKLM\software\microsoft\tracing\svchost_raschap[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\svchost_raschap[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\svchost_raschap[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\svchost_raschap[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\svchost_raschap[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\svchost_raschap[filedirectory]
Queries value: HKLM\software\microsoft\tracing\oneexsup[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\oneexsup[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\oneexsup[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\oneexsup[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\oneexsup[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\oneexsup[filedirectory]
Queries value: HKLM\software\microsoft\tracing\wlpolicy[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\wlpolicy[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\wlpolicy[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\wlpolicy[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\wlpolicy[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\wlpolicy[filedirectory]
Queries value: HKLM\software\microsoft\tracing\ipnathlp[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\ipnathlp[filetracingmask]
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
Queries value: HKLM\software\microsoft\com3[regdbversion]
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: HKLM\software\microsoft\tracing\ipnathlp[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\ipnathlp[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\ipnathlp[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\ipnathlp[filedirectory]
Queries value: HKLM\software\microsoft\tracing\dot3api[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\dot3api[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\dot3api[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\dot3api[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\dot3api[maxfilesize]
Queries value: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprocserver32[]
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: HKLM\software\microsoft\tracing\dot3api[filedirectory]
Queries value: HKLM\software\microsoft\tracing\netman[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\netman[filetracingmask]
Queries value: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}[appid]
Queries value: HKCR\appid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}[dllsurrogate]
Queries value: HKLM\software\microsoft\tracing\netman[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\netman[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\netman[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\netman[filedirectory]
Queries value: HKLM\software\microsoft\tracing\rasdlg[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\rasdlg[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\rasdlg[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\rasdlg[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\rasdlg[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\rasdlg[filedirectory]
Queries value: HKLM\system\currentcontrolset\control\productoptions[producttype]
Queries value: HKLM\software\microsoft\windows\currentversion\telephony[tapisrvwaithint]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling[explorer.exe]
Queries value: HKLM\software\microsoft\windows\currentversion\telephony[min]
Queries value: HKLM\software\microsoft\windows\currentversion\telephony[tapiscpttl]
Queries value: HKLM\software\microsoft\windows\currentversion\telephony[max]
Queries value: HKLM\software\microsoft\windows\currentversion\telephony[rpctimeout]
Queries value: HKLM\software\microsoft\windows\currentversion\telephony[domainname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
Queries value: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\windows\currentversion\telephony[tapisrvnumhandlebuckets]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
Queries value: HKLM\system\currentcontrolset\services\tapisrv\parameters[servicedllunloadonstop]
Queries value: HKLM\system\currentcontrolset\services\rasman\parameters[servicedll]
Queries value: HKLM\system\currentcontrolset\services\rasman\parameters[servicemain]
Queries value: HKLM\system\currentcontrolset\services\rasman\parameters[allowexternalcallers]
Queries value: HKLM\system\currentcontrolset\services\rasman\parameters[prohibitipsec]
Queries value: HKLM\system\currentcontrolset\services\rasman\parameters[ipoutlowwatermark]
Queries value: HKLM\system\currentcontrolset\services\rasman\parameters[ipouthighwatermark]
Queries value: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}[appid]
Queries value: HKLM\software\policies\microsoft\internet explorer\security[disablesecuritysettingscheck]
Queries value: HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\inprocserver32[inprocserver32]
Queries value: HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[dllsurrogate]
Queries value: HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[localservice]
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: HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\inprocserver32[]
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: HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[]
Queries value: HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[serviceparameters]
Queries value: HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[runas]
Queries value: HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[activateatstorage]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
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[filterclusterip]
Queries value: HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}[appid]
Queries value: HKLM\system\currentcontrolset\control\network[config]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}[description]
Queries value: HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[launchpermission]
Queries value: HKLM\software\microsoft\ole[legacyauthenticationlevel]
Queries value: HKLM\software\microsoft\ole[legacyimpersonationlevel]
Queries value: HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[authenticationlevel]
Queries value: HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[remoteservername]
Queries value: HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[srptrustlevel]
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[queryipmatching]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
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\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[svchost.exe]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi[clsid]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi[service]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi[coservices]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi[bindform]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi[helptext]
Queries value:
HKU\.default\software\microsoft\windows\shellnoroam\muicache[@netcfgx.dll,-50001]
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\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi\interfaces[lowerrange]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi\interfaces[lowerexclude]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi\interfaces[upperrange]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi\interfaces[filtermediatypes]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
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[multicastlistenlevel]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[enabledhcp]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[leaseobtainedtime]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[leaseterminatestime]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpserver]
Queries value: HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\inprocserver32[inprocserver32]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
Queries value: HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\inprocserver32[]
Queries value: HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}[appid]
Queries value: HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[debugsurrogate]
Queries value: HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\inprocserver32[]
Queries value: HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}[appid]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[primarymodule]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[eventmessagefile]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system\service control manager[categorymessagefile]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system\service control manager[parametermessagefile]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system\service control manager[eventmessagefile]
Queries value: HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\inprocserver32[threadingmodel]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0001[description]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0001\ndi[clsid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0001\ndi[service]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0001\ndi[coservices]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0001\ndi[bindform]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[wmiprvse.exe]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0001\ndi[helptext]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0001\ndi\interfaces[lowerrange]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0001\ndi\interfaces[lowerexclude]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0001\ndi\interfaces[upperrange]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0001\ndi\interfaces[filtermediatypes]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[maxnumberofaddressestoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[domain]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008[description]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008\ndi[clsid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008\ndi[service]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008\ndi[coservices]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008\ndi[bindform]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008\ndi[helptext]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpdomain]
Queries value: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprocserver32[]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008\ndi\interfaces[lowerrange]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008\ndi\interfaces[lowerexclude]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008\ndi\interfaces[upperrange]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0008\ndi\interfaces[filtermediatypes]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[ipautoconfigurationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[addresstype]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpnameserver]
Queries value: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}[appid]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[nameserver]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[ipenablerouter]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableicmpredirect]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[deadgwdetectdefault]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dontadddefaultgatewaydefault]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d597862O-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d597862O-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\{d597862O-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\{d597862O-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\{d597862O-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\{d597862O-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\{d597862O-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\{d597862O-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\{d597862O-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\{d597862O-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\{d597862O-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\{d597862O-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\{d597862O-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\{d597862O-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\{d597862O-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\{d597862O-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\{d597862O-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[allowperusermoniker]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enablesecurityfilters]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\adapters\ndiswanip[numinterfaces]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\adapters\ndiswanip[ipinterfaces]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[ipaddress]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[subnetmask]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
Queries value: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}\typelib[]
Queries value: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}\typelib[version]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[defaultgateway]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[defaultgatewaymetric]
Queries value: HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}\2.0\0\win32[]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[interfacemetric]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[tcpallowedports]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[udpallowedports]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[rawipallowedprotocols]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[activeconfigurations]
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: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{d789ab02-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberclsid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{d789ab02-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[active]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{d789ab02-5b9f-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}\subscriptions\{d789ab02-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassid]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}[description]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi[clsid]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi[service]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi[coservices]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi[bindform]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi[helptext]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi\interfaces[lowerrange]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi\interfaces[lowerexclude]
Queries value:
HKLM\system\currentcontrolset\control\computername\computername[computername]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi\interfaces[upperrange]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi\interfaces[filtermediatypes]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberclsid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[active]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[methodname]
Queries value: HKLM\system\currentcontrolset\services\netbt\parameters[enablelmhosts]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[interfaceid]
Queries value:
HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{16325b0b-4636-4303-abe3-c7d49d7cecdc}[nameserverlist]
Queries value:
HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{16325b0b-4636-4303-abe3-c7d49d7cecdc}[netbiosoptions]
Queries value: HKLM\system\currentcontrolset\services\rasman\parameters[medias]
Queries value: HKLM\software\microsoft\tracing\rastapi[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\rastapi[filetracingmask]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[eventclasspartitionid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{1ec466dd-2b44-4231-a775-cbd69f6eb46b}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberclsid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{1ec466dd-2b44-4231-a775-cbd69f6eb46b}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[subscribermoniker]
Queries value: HKLM\software\microsoft\tracing\rastapi[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\rastapi[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\rastapi[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\rastapi[filedirectory]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{1ec466dd-2b44-4231-a775-cbd69f6eb46b}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[active]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{1ec466dd-2b44-4231-a775-cbd69f6eb46b}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{1ec466dd-2b44-4231-a775-cbd69f6eb46b}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassid]

Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{4d99c768-0774-4b40-ac15-8342c658aad1}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberclsid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{4d99c768-0774-4b40-ac15-8342c658aad1}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[subscribermoniker]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{4d99c768-0774-4b40-ac15-8342c658aad1}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[active]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{4d99c768-0774-4b40-ac15-8342c658aad1}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{4d99c768-0774-4b40-ac15-8342c658aad1}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{68b25be9-46e1-45c1-8062-41b3d17a79a0}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberclsid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{68b25be9-46e1-45c1-8062-41b3d17a79a0}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[subscribermoniker]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{68b25be9-46e1-45c1-8062-41b3d17a79a0}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[active]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{68b25be9-46e1-45c1-8062-41b3d17a79a0}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{68b25be9-46e1-45c1-8062-41b3d17a79a0}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{6b9c1fb5-c711-47f3-94f9-bac5ad5535fe}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberclsid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{6b9c1fb5-c711-47f3-94f9-bac5ad5535fe}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[subscribermoniker]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{6b9c1fb5-c711-47f3-94f9-bac5ad5535fe}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[active]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{6b9c1fb5-c711-47f3-94f9-bac5ad5535fe}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{6b9c1fb5-c711-47f3-94f9-bac5ad5535fe}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{7f7b0a42-f639-4f28-9cf7-9338fedc54f0}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberclsid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{7f7b0a42-f639-4f28-9cf7-9338fedc54f0}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[subscribermoniker]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{7f7b0a42-f639-4f28-9cf7-9338fedc54f0}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[active]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{7f7b0a42-f639-4f28-9cf7-9338fedc54f0}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{7f7b0a42-f639-4f28-9cf7-9338fedc54f0}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{913b976b-c04f-4957-90ef-c1ee4d66edfc}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberclsid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{913b976b-c04f-4957-90ef-c1ee4d66edfc}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[subscribermoniker]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{913b976b-c04f-4957-90ef-c1ee4d66edfc}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[active]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{913b976b-c04f-4957-90ef-c1ee4d66edfc}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{913b976b-c04f-4957-90ef-c1ee4d66edfc}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassid]
Queries value: HKLM\software\microsoft\tracing\tapi32[enabledebuggertracing]
Queries value: HKLM\software\microsoft\tracing\tapi32[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\tapi32[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\tapi32[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\tapi32[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\tapi32[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\tapi32[filedirectory]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{a637889b-9e0a-4dc0-8316-d42b20771b16}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberclsid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{a637889b-9e0a-4dc0-8316-d42b20771b16}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[subscribermoniker]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{a637889b-9e0a-4dc0-8316-d42b20771b16}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[active]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{a637889b-9e0a-4dc0-8316-d42b20771b16}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{a637889b-9e0a-4dc0-8316-d42b20771b16}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\subscriptions\{b8808a2b-4188-47e6-85ae-d3e76088cdae}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberclsid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-

00805fc79216}\subscriptions\{b8808a2b-4188-47e6-85ae-d3e76088cdae}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscribermoniker]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{b8808a2b-4188-47e6-85ae-d3e76088cdae}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[active]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{b8808a2b-4188-47e6-85ae-d3e76088cdae}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{b8808a2b-4188-47e6-85ae-d3e76088cdae}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscriptionid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscriptionname]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[peruser]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[ownersid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[enabled]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[description]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[machinename]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[filtercriteria]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscribermoniker]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassapplicationid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberpartitionid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberapplicationid]
Queries value:
HKU\.default\software\microsoft\windows\currentversion\telephony\handoffpriorities[requestmakecall]
Queries value:
HKU\.default\software\microsoft\windows\currentversion\telephony\handoffpriorities[requestmediacall]
Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[numproviders]
Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerid0]
Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerfilename0]
Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerid1]
Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerfilename1]
Queries value: HKLM\software\microsoft\tracing\kmddsp[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\kmddsp[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\kmddsp[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\kmddsp[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\kmddsp[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\kmddsp[filedirectory]
Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerid2]
Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerfilename2]
Queries value: HKLM\software\microsoft\tracing\ndptsp[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\ndptsp[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\ndptsp[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\ndptsp[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\ndptsp[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\ndptsp[filedirectory]
Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerid3]
Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerfilename3]
Queries value: HKLM\software\microsoft\tracing\conftsp[enabledebuggertracing]
Queries value: HKLM\software\microsoft\tracing\conftsp[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\conftsp[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\conftsp[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\conftsp[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\conftsp[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\conftsp[filedirectory]
Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerid4]
Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerfilename4]
Queries value: HKLM\software\microsoft\windows\currentversion\h323tsp[debuglevel]
Queries value: HKLM\software\microsoft\windows\currentversion\h323tsp[q931listenport]
Queries value:
HKLM\software\microsoft\windows\currentversion\h323tsp[q931alertingtimeout]
Queries value:
HKLM\software\microsoft\windows\currentversion\h323tsp[h323gatewayaddress]
Queries value:
HKLM\software\microsoft\windows\currentversion\h323tsp[h323gatewayenabled]
Queries value: HKLM\software\microsoft\windows\currentversion\h323tsp[h323proxyaddress]

Queries value: HKLM\software\microsoft\windows\currentversion\h323tsp[h323proxyenabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\h323tsp[h323gatekeeperenabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\h323tsp[h323gklogonphonenumberenabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\h323tsp[h323gklogonaccountnameenabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerid5]
Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerfilename5]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0000[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0001[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0002[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0003[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006[wanendpoints]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006[enableforras]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006[enableforrouting]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006[enableforoutboundrouting]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006[minwanendpoints]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006[maxwanendpoints]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006[driverdesc]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006[fclientrole]
Queries value:
HKLM\system\currentcontrolset\services\rasman\parameters[limitsimultaneousincomingcalls]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006[calledidinformation]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005[wanendpoints]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005[enableforras]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005[enableforrouting]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005[enableforoutboundrouting]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005[minwanendpoints]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005[maxwanendpoints]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005[driverdesc]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005[fclientrole]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005[calledidinformation]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004[wanendpoints]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004[enableforras]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004[enableforrouting]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004[enableforoutboundrouting]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004[minwanendpoints]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004[maxwanendpoints]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004[driverdesc]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004[fclientrole]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004[calledidinformation]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007[wanendpoints]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007[enableforras]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007[enableforrouting]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007[enableforoutboundrouting]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007[minwanendpoints]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007[maxwanendpoints]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007[driverdesc]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007[fclientrole]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007[calledidinformation]

Queries value: HKLM\system\currentcontrolset\services\rasman\parameters[numberofrings]
Queries value:
HKLM\system\currentcontrolset\services\rasman\parameters\quarantine[enabled]
Queries value: HKLM\software\microsoft\tracing\rasqec[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\rasqec[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\rasqec[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\rasqec[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\rasqec[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\rasqec[filedirectory]
Queries value: HKLM\software\microsoft\tracing\rasman[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\rasman[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\rasman[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\rasman[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\rasman[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\rasman[filedirectory]
Queries value:
HKLM\system\currentcontrolset\services\rasman\parameters\quarantine[autorefreshenabled]
Queries value: HKLM\software\microsoft\tracing\ppp[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\ppp[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\ppp[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\ppp[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\ppp[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\ppp[filedirectory]
Queries value: HKLM\software\microsoft\tracing\bap[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\bap[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\bap[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\bap[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\bap[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\bap[filedirectory]
Queries value: HKLM\system\currentcontrolset\services\rasman\ppp[maxterminate]
Queries value: HKLM\system\currentcontrolset\services\rasman\ppp[maxconfigure]
Queries value: HKLM\system\currentcontrolset\services\rasman\ppp[maxfailure]
Queries value: HKLM\system\currentcontrolset\services\rasman\ppp[maxreject]
Queries value: HKLM\system\currentcontrolset\services\rasman\ppp[restarttimer]
Queries value: HKLM\system\currentcontrolset\services\rasman\ppp[negotiatetime]
Queries value: HKLM\system\currentcontrolset\services\rasman\ppp[defaultcallbackdelay]
Queries value: HKLM\system\currentcontrolset\services\rasman\ppp[defaultportlimit]
Queries value: HKLM\system\currentcontrolset\services\rasman\ppp[defaultsessiontimeout]
Queries value: HKLM\system\currentcontrolset\services\rasman\ppp[defaultidletimeout]
Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp[lowerbandwidththreshold]
Queries value: HKLM\system\currentcontrolset\services\rasman\ppp[timebelowtheshold]
Queries value: HKLM\system\currentcontrolset\services\rasman\ppp[baplistentimeout]
Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp[unknownpackettracesize]
Queries value: HKLM\system\currentcontrolset\services\rasman\ppp[echorequestinterval]
Queries value: HKLM\system\currentcontrolset\services\rasman\ppp[idletimebeforeecho]
Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp[missedechosbeforedisconnect]
Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp[dontnegotiatemultilinkonsinglelink]
Queries value: HKLM\system\currentcontrolset\services\rasman\ppp[parsedllpath]
Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[path]
Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[negotiateipcp]
Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[negotiatebacp]
Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[negotiatecbcp]
Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[negotiateccp]
Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[negotiateeap]
Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[negotiateipx]
Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[negotiatepap]
Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[negotiateatcp]
Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[negotiatespap]
Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\chap[path]
Queries value: HKLM\software\microsoft\tracing\rasspap[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\rasspap[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\rasspap[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\rasspap[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\rasspap[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\rasspap[filedirectory]
Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[followstrictsequencing]
Queries value: HKLM\software\microsoft\tracing\raspap[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\raspap[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\raspap[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\raspap[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\raspap[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\raspap[filedirectory]
Queries value: HKLM\software\microsoft\tracing\raseap[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\raseap[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\raseap[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\raseap[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\raseap[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\raseap[filedirectory]
Queries value: HKLM\system\currentcontrolset\services\rasman\ppp\eap\13[path]
Queries value: HKLM\system\currentcontrolset\services\rasman\ppp\eap\25[path]
Queries value: HKLM\system\currentcontrolset\services\rasman\ppp\eap\26[path]
Queries value: HKLM\system\currentcontrolset\services\rasman\ppp\eap\4[path]
Queries value: HKLM\software\microsoft\tracing\rasccp[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\rasccp[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\rasccp[enableconsoletracing]

Queries value: HKLM\software\microsoft\tracing\rasccp[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\rasccp[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\rasccp[filedirectory]
Queries value: HKLM\software\microsoft\tracing\rasbacp[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\rasbacp[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\rasbacp[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\rasbacp[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\rasbacp[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\rasbacp[filedirectory]
Queries value: HKLM\software\microsoft\tracing\rasiphlp[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\rasiphlp[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\rasiphlp[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\rasiphlp[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\rasiphlp[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\rasiphlp[filedirectory]
Queries value: HKLM\software\microsoft\rpc\securityservice[10]
Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]
Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]
Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[version]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]
Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]
Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]
Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment]
Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type]
Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize]
Queries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[usedhcpaddressing]
Queries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[networkadapterguid]
Queries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[suppresswinsnameservers]
Queries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[suppressdnsnameservers]
Queries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[initialaddresspoolsize]
Queries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[allownetworkaccess]
Queries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[winsnameserver]
Queries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[winsnameserverbackup]
Queries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[dnsnameservers]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\adapters\ndiswanip[ipconfig]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4fe87b73-b12e-47d6-82c4-
fb0d4cf73262}[dhcpipaddress]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4fe87b73-b12e-47d6-82c4-
fb0d4cf73262}[dhcpsubnetmask]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4fe87b73-b12e-47d6-82c4-
fb0d4cf73262}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4fe87b73-b12e-47d6-82c4-
fb0d4cf73262}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{4fe87b73-b12e-47d6-
82c4-fb0d4cf73262}[nameserverlist]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{cac79791-bd6d-4f3e-bcad-
e3686652faee}[dhcpipaddress]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{cac79791-bd6d-4f3e-bcad-
e3686652faee}[dhcpsubnetmask]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{cac79791-bd6d-4f3e-bcad-
e3686652faee}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{cac79791-bd6d-4f3e-bcad-
e3686652faee}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{cac79791-bd6d-4f3e-
bcad-e3686652faee}[nameserverlist]
Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[maxmsipcpoptioncfgcnt]
Queries value: HKLM\software\microsoft\tracing\rasipcp[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\rasipcp[filetracingmask]

Queries value: HKLM\software\microsoft\tracing\rasipcp[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\rasipcp[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\rasipcp[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\rasipcp[filedirectory]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[spoolsv.exe]
Queries value:
HKLM\system\currentcontrolset\control\networkprovider\hworder[providerorder]
Queries value: HKLM\system\currentcontrolset\services\rdpnp\networkprovider[name]
Queries value: HKLM\system\currentcontrolset\services\rdpnp\networkprovider[class]
Queries value:
HKLM\system\currentcontrolset\services\rdpnp\networkprovider[providerpath]
Queries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider[name]
Queries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider[class]
Queries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider[providerpath]
Queries value: HKLM\system\currentcontrolset\services\webclient\networkprovider[name]
Queries value: HKLM\system\currentcontrolset\services\webclient\networkprovider[class]
Queries value:
HKLM\system\currentcontrolset\services\webclient\networkprovider[providerpath]
Queries value: HKLM\software\microsoft\windows nt\currentversion\network\world full
access shared parameters[sort hyphens]
Queries value: HKLM\software\microsoft\wbem\cimom[logging]
Queries value: HKLM\software\microsoft\wbem\cimom[log file max size]
Queries value: HKCR\clsid\{4fa18276-912a-11d1-ad9b-
00c04fd8fdff}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\inprocserver32[]
Queries value: HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}[appid]
Queries value: HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-
5e7582d8c9fa}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\inprocserver32[]
Queries value: HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}[appid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\perflib[disable
performance counters]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[jqs.exe]
Queries value: HKLM\software\microsoft\wbem\cimom[working directory]
Queries value: HKLM\system\currentcontrolset\control\session
manager\appcompatibility[disableappcompat]
Queries value: HKCU\appevents\schemes\apps\.default\systemnotification\.current[]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[wmiadap]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[wmiadap]
Queries value: HKLM\software\microsoft\wbem\cimom[logging directory]
Queries value: HKLM\software\microsoft\wbem\cimom[repository directory]
Queries value: HKU\.default\control panel\international[locale]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
Queries value: HKU\.default\control panel\international[scurrency]
Queries value: HKU\.default\control panel\international[smondecimalsep]
Queries value: HKU\.default\control panel\international[smonthousandsep]
Queries value: HKU\.default\control panel\international[smongrouping]
Queries value: HKU\.default\control panel\international[spositivesign]
Queries value: HKU\.default\control panel\international[snegativesign]
Queries value: HKU\.default\control panel\international[icurrdigits]
Queries value: HKU\.default\control panel\international[sdecimal]
Queries value: HKU\.default\control panel\international[sthousand]
Queries value: HKU\.default\control panel\international[sgrouping]
Queries value: HKU\.default\control panel\international[s1159]
Queries value: HKU\.default\control panel\international[s2359]
Queries value: HKU\.default\control panel\international[sshortdate]
Queries value: HKU\.default\control panel\international[slongdate]
Queries value: HKU\.default\control panel\international[stimeformat]
Queries value: HKU\.default\control panel\international[icalendartype]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
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 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: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
Queries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]

Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
Queries value: HKU\.default\software\microsoft\multimedia\audio[systemformats]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.imaadpcm]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msadpcm]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msg711]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msgsm610]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.trspch]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msg723]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msaudio1]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.sl_anet]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.l3acm]
Queries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[fdwsupport]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cformattags]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[aformattagcache]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags]
Queries value: HKU\.default\software\microsoft\multimedia\audio compression
manager\msacm[nopcmconverter]
Queries value: HKU\.default\software\microsoft\multimedia\audio compression
manager\priority v4.00[priority1]
Queries value: HKU\.default\control panel\desktop[smoothscroll]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\winlogon[chkaccdebuglevel]
Queries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[personal]
Queries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[local settings]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\winlogon[rsopdebuglevel]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
Queries value:
HKU\.default\software\microsoft\windows\currentversion\thememanager[compositing]
Queries value: HKU\.default\control panel\desktop[lamebuttontext]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[wmiadap.exe]
Queries value: HKLM\software\microsoft\ole[maximumallowedallocationsize]
Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
Queries value: HKLM\software\microsoft\wbem\cimom[adapperflibmaxsizeblobcollect]
Queries value: HKLM\software\microsoft\wbem\cimom[processid]
Queries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
Queries value: HKLM\software\microsoft\com3[com+enabled]
Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]
Queries value: HKCR\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32[]
Queries value: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[appid]
Queries value: HKCR\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[appid]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[dllsurrogate]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[localservice]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[serviceparameters]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[runas]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[activateatstorage]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[launchpermission]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[authenticationlevel]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[remoteservername]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[srptrustlevel]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[debugsurrogate]
Queries value: HKCR\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[]
Queries value: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[appid]
Queries value: HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32[]
Queries value: HKCR\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[threadingmodel]
Queries value: HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32[]
Queries value: HKCR\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32[]
Queries value: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[appid]
Queries value: HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32[]
Queries value: HKCR\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\wbem\cimom[enableprivateobjectheap]
Queries value: HKLM\software\microsoft\wbem\cimom[contextlimit]
Queries value: HKLM\software\microsoft\wbem\cimom[objectlimit]
Queries value: HKLM\software\microsoft\wbem\cimom[identifierlimit]
Queries value: HKCR\clsid\{cd1abfc8-6c5e-4a8d-b90b-
2a3b153b886d}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{cd1abfc8-6c5e-4a8d-b90b-2a3b153b886d}\inprocserver32[]
Queries value: HKCR\clsid\{cd1abfc8-6c5e-4a8d-b90b-2a3b153b886d}[appid]
Queries value: HKCR\clsid\{9a653086-174f-11d2-b5f9-
00104b703efd}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{9a653086-174f-11d2-b5f9-00104b703efd}\inprocserver32[]
Queries value: HKCR\clsid\{9a653086-174f-11d2-b5f9-00104b703efd}[appid]
Queries value: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32[]
Queries value: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}[appid]
Queries value: HKCR\interface\{027947e1-d731-11ce-a357-000000000001}\proxystubclsid32[]
Queries value: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[threadingmodel]
Queries value: HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}\proxystubclsid32[]
Queries value: HKCR\clsid\{cc9072ab-c000-49d8-a5aa-
00266c8dbb9b}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{cc9072ab-c000-49d8-a5aa-00266c8dbb9b}\inprocserver32[]
Queries value: HKCR\clsid\{cc9072ab-c000-49d8-a5aa-00266c8dbb9b}[appid]
Queries value: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32[]
Queries value: HKCR\clsid\{d2d588b5-d081-11d0-99e0-
00c04fc2f8ec}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{d2d588b5-d081-11d0-99e0-
00c04fc2f8ec}\inprocserver32[synchronization]
Queries value: HKCR\clsid\{d2d588b5-d081-11d0-99e0-00c04fc2f8ec}\inprocserver32[]
Queries value: HKCR\clsid\{d2d588b5-d081-11d0-99e0-00c04fc2f8ec}[]
Queries value: HKCR\clsid\{d2d588b5-d081-11d0-99e0-00c04fc2f8ec}[appid]

Queries value: HKCR\clsid\{eac8a024-21e2-4523-ad73-a71a0aa2f56a}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{eac8a024-21e2-4523-ad73-a71a0aa2f56a}\inprocserver32[]
Queries value: HKCR\clsid\{eac8a024-21e2-4523-ad73-a71a0aa2f56a}[appid]
Queries value: HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprocserver32[]
Queries value: HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}[appid]
Queries value: HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\inprocserver32[]
Queries value: HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}[appid]
Queries value: HKCR\clsid\{eac8a024-21e2-4523-ad73-a71a0aa2f56a}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{d2d588b5-d081-11d0-99e0-00c04fc2f8ec}\inprocserver32[inprocserver32]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[b48d49a2-e777-11d0-a50c-00a0c9062910]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[b48d49a3-e777-11d0-a50c-00a0c9062910]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[05901221-d566-11d1-b2f0-00a0c9062910]
Queries value: HKLM\system\currentcontrolset\services\acpi[mofimagepath]
Queries value: HKLM\system\currentcontrolset\services\acpi[imagepath]
Queries value: HKLM\system\currentcontrolset\services\mssmbios[mofimagepath]
Queries value: HKLM\system\currentcontrolset\services\mssmbios[imagepath]
Queries value: HKLM\system\currentcontrolset\services\pcnet[mofimagepath]
Queries value: HKLM\system\currentcontrolset\services\pcnet[imagepath]
Queries value: HKLM\system\currentcontrolset\services\ipnat[mofimagepath]
Queries value: HKLM\system\currentcontrolset\services\ipnat[imagepath]
Queries value: HKLM\system\currentcontrolset\services\http[mofimagepath]
Queries value: HKLM\system\currentcontrolset\services\http[imagepath]
Queries value: HKCR\clsid\{c10b4771-4da0-11d2-a2f5-00c04f86fb7d}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{c10b4771-4da0-11d2-a2f5-00c04f86fb7d}\inprocserver32[]
Queries value: HKCR\clsid\{c10b4771-4da0-11d2-a2f5-00c04f86fb7d}[appid]
Queries value: HKCR\clsid\{c10b4771-4da0-11d2-a2f5-00c04f86fb7d}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\wbem\cimom[enableprivatemofdheap]
Queries value: HKCR\clsid\{cb8555cc-9128-11d1-ad9b-00c04fd8fdff}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{cb8555cc-9128-11d1-ad9b-00c04fd8fdff}\inprocserver32[]
Queries value: HKCR\clsid\{cb8555cc-9128-11d1-ad9b-00c04fd8fdff}[appid]
Queries value: HKCR\clsid\{cb8555cc-9128-11d1-ad9b-00c04fd8fdff}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[unsecapp.exe]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[981f2d7e-b1f3-11d0-8dd7-00c04fc3358c]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[981f2d7d-b1f3-11d0-8dd7-00c04fc3358c]
Sets/Creates value: HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\calc.exe]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\run[1h6wzb8f9vux2v7xspnwvurp]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonintranet]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[1409]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[1409]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[1409]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[1409]
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]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]
Value changes: HKCU\sessioninformation[programcount]
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\zones\0[1609]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[1406]
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[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[1609]

Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[1406]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\1[1406]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\2[1406]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\3[1406]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\4[1406]
Value changes: HKCU\software\microsoft\internet explorer\phishingfilter[enabledv8]
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[history]
Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell folders[common appdata]
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[appdata]
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[globaluseroffline]
Value changes: HKLM\system\currentcontrolset\services\eventlog\application\microsoft h.323 telephony service provider[eventmessagefile]
Value changes: HKLM\system\currentcontrolset\services\eventlog\application\microsoft h.323 telephony service provider[typessupported]
Value changes: HKLM\software\microsoft\wbem\wdm[c:\windows\system32\advapi32.dll[mofresourcename]]