Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 2, Task ID: 2

Task ID:	2
Risk Level:	10
Date Processed:	2016-03-02 17:52:12 (UTC)
Processing Time:	63.32 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\spyeye_injector.exe"
Sample ID:	2
Type:	basic
Owner:	admin
Label:	spyeye_injector.exe
Date Added:	2016-03-02 17:52:11 (UTC)
File Type:	PE32:win32:gui
File Size:	103936 bytes
MD5:	b98bb6d7428c3dbffcfcab2414c6daa2
SHA256:	fc7f54ce456c164452d8429a7fd5f52629a69338f8954e287d2664c03c37e029
Description:	None

Pattern Matching Results

4 Terminates process under Windows subfolder
10 Creates malicious mutex: Spyeye [Banking]
6 Modifies registry autorun entries
5 Abnormal sleep detected
10 Suspicious writeprocess: Spyeye [Banking]
5 Packer: UPX
6 Notifies system about Internet connection change
5 Adds autostart object
4 Reads process memory
2 PE: Nonstandard section
6 Renames file on boot
5 PE: Contains compressed section
3 Program causes a crash [Info]
7 Writes to memory of system processes

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\83A49421955.exe ["C:\WinOldFileq\83A49421955.exe"]
Creates process: C:\Users\Admin\AppData\Local\Temp\W2X5C34.exe ["C:\Users\Admin\AppData\Local\Temp\W2X5C34.exe"]
Creates process: c:\windows\SysWOW64\calc.exe ["c:\windows\system32\calc.exe"]
Creates process: C:\Windows\SysWOW64\rundll32.exe ["C:\Windows\system32\rundll32.exe" "C:\Windows\syswow64\WININET.dll",DispatchAPICall 1]
Reads from process: PID:1092 C:\Windows\explorer.exe
Reads from process: PID:376 C:\Windows\System32\psxss.exe
Reads from process: PID:420 C:\Windows\System32\winlogon.exe
Reads from process: PID:428 C:\Windows\System32\wininit.exe
Reads from process: PID:500 C:\Windows\System32\lsass.exe
Reads from process: PID:508 C:\Windows\System32\lsm.exe
Reads from process: PID:608 C:\Windows\System32\svchost.exe
Reads from process: PID:676 C:\Windows\System32\svchost.exe
Reads from process: PID:724 C:\Windows\System32\svchost.exe
Reads from process: PID:884 C:\Windows\System32\svchost.exe
Reads from process: PID:988 C:\Windows\System32\svchost.exe
Reads from process: PID:272 C:\Windows\System32\svchost.exe
Reads from process: PID:1072 C:\Windows\System32\dwm.exe
Reads from process: PID:1124 C:\Windows\System32\taskhost.exe
Reads from process: PID:1328 C:\Windows\System32\svchost.exe
Reads from process: PID:1452 C:\Windows\System32\svchost.exe
Reads from process: PID:1564 C:\Windows\System32\spoolsv.exe
Reads from process: PID:1600 C:\Windows\System32\svchost.exe
Reads from process: PID:1620 C:\Windows\System32\CISVC.EXE
Reads from process: PID:1692 C:\Program Files (x86)\EMET 5.2\EMET_Service.exe
Reads from process: PID:1752 C:\Windows\System32\svchost.exe
Reads from process: PID:1788 C:\Windows\System32\inetsrv\inetinfo.exe
Reads from process: PID:1836 C:\Windows\System32\svchost.exe
Reads from process: PID:1872 C:\Windows\System32\svchost.exe
Reads from process: PID:1908 C:\Windows\System32\mqsvc.exe
Reads from process: PID:1960 C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe
Reads from process: PID:1968 C:\Program Files (x86)\EMET 5.2\EMET_Agent.exe
Reads from process: PID:800 C:\Windows\System32\TCPSVCS.EXE

Reads from process:	PID:704 C:\Windows\System32\tlntsrv.exe
Reads from process:	PID:1208 C:\Windows\System32\svchost.exe
Reads from process:	PID:1800 C:\Windows\System32\mqtgsvc.exe
Reads from process:	PID:2072 C:\Windows\System32\nfsclnt.exe
Reads from process:	PID:2224 C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe
Reads from process:	PID:2444 C:\Windows\System32\UIODetect.exe
Reads from process:	PID:2548 C:\Windows\System32\svchost.exe
Reads from process:	PID:3008 C:\Windows\System32\sdclt.exe
Reads from process:	PID:3044 C:\Windows\System32\taskhost.exe
Reads from process:	PID:2816 C:\Windows\System32\ivm\ivm-service.exe
Reads from process:	PID:2856 C:\Windows\System32\wbem\unsecapp.exe
Reads from process:	PID:2596 C:\Windows\System32\wbem\WmiPrvSE.exe
Reads from process:	PID:2068 C:\Windows\System32\conhost.exe
Writes to process:	PID:1428 C:\Program Files (x86)\Adobe\Reader 9.0\Reader\reader_sl.exe
Writes to process:	PID:2944 C:\Windows\System32\paranormal.exe
Writes to process:	PID:2328 C:\Users\Admin\AppData\Local\Temp\W2X5C34.exe
Writes to process:	PID:2456 C:\Windows\Temp\spyeye_injector.exe
Writes to process:	PID:416 C:\Windows\SysWOW64\calc.exe
Writes to process:	PID:2712 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2504 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:540 C:\Windows\SysWOW64\rundll32.exe
Terminates process:	C:\WinOldFileq\83A49421955.exe
Terminates process:	C:\Windows\Temp\spyeye_injector.exe
Terminates process:	C:\Windows\SysWOW64\calc.exe
Terminates process:	C:\Windows\SysWOW64\WerFault.exe
Terminates process:	C:\Windows\SysWOW64\rundll32.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\BaseNamedObjects\RPCController
Creates mutex:	\Sessions\1\BaseNamedObjects\zXeRY3a_PtW|00000000
Creates mutex:	\Sessions\1\BaseNamedObjects_!MSFTHISTORY!_
Creates mutex:	\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!temporary internet files!content.ie5!
Creates mutex:	\BaseNamedObjects\B9EXF6TTcUY9ZFyZ98DUzD85UB59cpO
Creates mutex:	\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!roaming!microsoft!windows!cookies!
Creates mutex:	\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!history!history.ie5!
Creates mutex:	\Sessions\1\BaseNamedObjects\WininetStartupMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\WininetConnectionMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\WininetProxyRegistryMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\RasPbFile
Creates mutex:	\Sessions\1\BaseNamedObjects\IESQMMUTEX_0_208
Creates mutex:	\Sessions\1\BaseNamedObjects\ZonesCounterMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\!IETld!Mutex
Creates mutex:	\Sessions\1\BaseNamedObjects_!MSFTHISTORY!_LOW!_
Creates mutex:	\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!temporary internet files!low!content.ie5!
Creates mutex:	\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!roaming!microsoft!windows!cookies!low!
Creates mutex:	\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!history!low!history.ie5!
Creates event:	\BaseNamedObjects\SvcctrlStartEvent_A3752DX
Creates event:	\Security\LSA_AUTHENTICATION_INITIALIZED
Creates event:	\BaseNamedObjects\ParanormalNotBusy
Creates event:	\KernelObjects\SystemErrorPortReady
Creates event:	\BaseNamedObjects\BFE_Notify_Event_{8053f4a8-1d1d-48e0-9163-ccc4c801b7f6}
Creates event:	\KernelObjects\MaximumCommitCondition

File System Events

Creates:	C:\WinOldFileq
Creates:	C:\WinOldFileq\
Creates:	C:\WinOldFileq\83A49421955.exe
Creates:	C:\WinOldFileq\DA9832AC502FF73
Creates:	C:\Users\Admin\AppData\Local\Temp\
Creates:	C:\Users\Admin\AppData\Local\Temp\W2X5C34.tmp
Creates:	C:\Users\Admin\AppData\Local\Temp\W2X5C34.exe
Creates:	C:\Users\Admin
Creates:	C:\Users\Admin\AppData\Local
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
Creates:	C:\Users\Admin\AppData\Roaming
Creates:	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\History
Creates:	C:\Users\Admin\Favorites
Creates:	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE

Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache
Opens: C:\Windows
Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\System32\wow64win.dll
Opens: C:\Windows\System32\wow64cpu.dll
Opens: C:\Windows\system32\wow64log.dll
Opens: C:\Windows\SysWOW64
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\Windows\SysWOW64\kernel32.dll
Opens: C:\
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\SysWOW64\ntdll.dll
Opens: C:\WinOldFileq
Opens: C:\WinOldFileq\
Opens: C:\Windows\Temp\spyeye_injector.exe
Opens: C:\WinOldFileq\83A49421955.exe
Opens: C:\Windows\SysWOW64\embdtrst.dll
Opens: C:\Windows\SysWOW64\apphelp.dll
Opens: C:\Windows\AppPatch\sysmain.sdb
Opens: C:\WinOldFileq\ui\SwDRM.dll
Opens: C:\Windows\SysWOW64\imm32.dll
Opens: C:\WinOldFileq\MSIMG32.dll
Opens: C:\Windows\SysWOW64\msimg32.dll
Opens: C:\WinOldFileq\DA9832AC5O2FF73
Opens: C:\Users\Admin\AppData\Local\Temp
Opens: C:\Users\Admin\AppData\Local\Temp\W2X5C34.exe
Opens: C:\Users
Opens: C:\Users\Admin
Opens: C:\Users\Admin\AppData
Opens: C:\Users\Admin\AppData\Local
Opens: C:\Users\Admin\AppData\Local\Temp\ui\SwDRM.dll
Opens: C:\Users\Admin\AppData\Local\Temp\MSIMG32.dll
Opens: C:\Windows\SysWOW64\user32.dll
Opens: C:\Windows\SysWOW64\wininet.dll
Opens: C:\windows\temp\MSIMG32.dll
Opens: C:\Program Files (x86)\Adobe\Reader 9.0\Reader\MSIMG32.dll
Opens: C:\Users\Admin\AppData\Local\Temp\W2X5C34.exe.Local\
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
Opens: C:\Windows\WindowsShell.Manifest
Opens: C:\Users\Admin\AppData\Local\Temp\profapi.dll
Opens: C:\Windows\SysWOW64\profapi.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\desktop.ini
Opens: C:\Users\Admin\AppData\Roaming
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini
Opens: C:\Windows\SysWOW64\ws2_32.dll
Opens: C:\Windows\SysWOW64\advapi32.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
Opens: C:\Users\Admin\AppData\Local\Temp\USERENV.dll
Opens: C:\Windows\SysWOW64\userenv.dll
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs
Opens: C:\Windows\SysWOW64\crypt32.dll
Opens: C:\Windows\SysWOW64\tzres.dll
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
Opens: C:\Windows\SysWOW64\mswsock.dll
Opens: C:\Users\Admin\AppData\Local\Temp\ntmarta.dll
Opens: C:\Windows\SysWOW64\ntmarta.dll
Opens: C:\Users\Admin\AppData\Local\Temp\dnsapi.DLL
Opens: C:\Windows\SysWOW64\dnsapi.dll
Opens: C:\Users\Admin\AppData\Local\Temp\iphlpapi.DLL
Opens: C:\Windows\SysWOW64\IPHLPAPI.DLL
Opens: C:\Windows\SysWOW64\WSHTCPIP.DLL
Opens: C:\Users\Admin\AppData\Local\Temp\WINNSI.DLL

Opens: C:\Windows\SysWOW64\winnsi.dll
Opens: C:\windows\temp\spyeye_injector.exe
Opens: C:\Windows\SysWOW64\nlaapi.dll
Opens: C:\Windows\SysWOW64\winrnr.dll
Opens: C:\Windows\SysWOW64\pnrpnsp.dll
Opens: C:\Windows\SysWOW64\NapiNSP.dll
Opens: C:\Users\Admin\AppData\Local\Temp\dhcpcsvc6.DLL
Opens: C:\Windows\SysWOW64\dhcpcsvc6.dll
Opens: C:\Users\Admin\AppData\Local\Temp\dhcpcsvc.DLL
Opens: C:\Windows\SysWOW64\dhcpcsvc.dll
Opens: C:\Windows\System32\drivers\etc\hosts
Opens: C:\Windows\SysWOW64\calc.exe
Opens: C:\windows\SysWOW64\ui\SwDRM.dll
Opens: C:\Users\Admin\AppData\Local\Temp\rasadhlp.dll
Opens: C:\Windows\SysWOW64\rasadhlp.dll
Opens: C:\Users\Admin\AppData\Local\Temp\RASAPI32.dll
Opens: C:\Windows\SysWOW64\rasapi32.dll
Opens: C:\Users\Admin\AppData\Local\Temp\rasman.dll
Opens: C:\Windows\SysWOW64\rasman.dll
Opens: C:\Users\Admin\AppData\Local\Temp\rtutils.dll
Opens: C:\Windows\SysWOW64\rtutils.dll
Opens: C:\ProgramData\Microsoft\Network\Connections\Pbk\
Opens: C:\Windows\SysWOW64\ras
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk\
Opens: C:\Users\Admin\AppData\Local\Temp\sensapi.dll
Opens: C:\Windows\SysWOW64\SensApi.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows
Opens: C:\Users\Admin\AppData\Local\Microsoft
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\Low
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows
Opens: C:\Users\Admin\AppData\Roaming\Microsoft
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low
Opens: C:\Users\Admin\Favorites
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Virtualized
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE\Low
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache\Low
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache\Low
Opens: C:\Users\Admin\AppData\Local\Temp\Low
Opens: C:\Windows\SysWOW64\rundll32.exe
Opens: C:\Windows\SysWOW64\ui\SwDRM.dll
Opens: C:\Windows\SysWOW64\rpcss.dll
Opens: C:\Windows\SysWOW64\wship6.dll
Opens: C:\Windows\SysWOW64\FWPUCLNT.DLL
Opens: C:\Windows\SysWOW64\wer.dll
Opens: C:\Windows\Registration\R000000000004.clb
Opens: C:\Windows\SysWOW64\netprofm.dll
Opens: C:\Windows\SysWOW64\WerFault.exe.Local\
Opens: C:\Windows\SysWOW64\Faultrep.dll
Opens: C:\Windows\SysWOW64\en-US\WerFault.exe.mui
Opens: C:\Windows\SysWOW64\uxtheme.dll
Opens: C:\Users\Admin\AppData\Local\Temp\CRYPTSP.dll
Opens: C:\Windows\SysWOW64\cryptsp.dll
Opens: C:\Windows\SysWOW64\rsaenh.dll
Opens: C:\Users\Admin\AppData\Local\Temp\RpcRtRemote.dll
Opens: C:\Windows\SysWOW64\RpcRtRemote.dll
Opens: C:\Windows\SysWOW64\npmproxy.dll
Opens: C:\Users\Admin\AppData\Local\Temp\VERSION.dll
Opens: C:\Windows\SysWOW64\version.dll
Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@microsoft[2].txt
Opens: C:\Windows\AppPatch\AcLayers.dll
Opens: C:\Windows\SysWOW64\winspool.drv
Opens: C:\Windows\SysWOW64\mpr.dll
Opens: C:\Windows\AppPatch\acwow64.dll
Opens: C:\Windows\syswow64\WININET.dll.manifest
Opens: C:\Windows\SysWOW64\dwmapi.dll
Opens: C:\Windows\SysWOW64\rundll32.exe.Local\
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low\desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low\Content.IE5
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low\Content.IE5\desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\History.IE5
Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\History.IE5\desktop.ini

Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\index.dat
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\Low\index.dat
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\History.IE5\index.dat
Writes to: C:\WinOldFileq\83A49421955.exe
Writes to: C:\WinOldFileq\DA9832AC502FF73
Writes to: C:\Users\Admin\AppData\Local\Temp\W2X5C34.exe
Reads from: C:\Windows\SysWOW64\ntdll.dll
Reads from: C:\Windows\Temp\spyeye_injector.exe
Reads from: C:\WinOldFileq\83A49421955.exe
Reads from: C:\WinOldFileq\DA9832AC502FF73
Reads from: C:\Users\Admin\AppData\Local\Temp\W2X5C34.exe
Reads from: C:\Windows\SysWOW64\user32.dll
Reads from: C:\Windows\SysWOW64\wininet.dll
Reads from: C:\Windows\SysWOW64\ws2_32.dll
Reads from: C:\Windows\SysWOW64\advapi32.dll
Reads from: C:\Windows\SysWOW64\crypt32.dll
Reads from: C:\Windows\System32\drivers\etc\hosts
Reads from: C:\Windows\SysWOW64\calc.exe
Reads from: C:\Windows\SysWOW64\rundll32.exe
Reads from: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@microsoft[2].txt
Deletes: C:\Windows\Temp\spyeye_injector.exe

Network Events

DNS query: alexeyartemov.com
DNS query: www.microsoft.com
Connects to: 88.198.13.147:443
Sends data to: 8.8.8.8:53
Sends data to: 4.2.2.1:53

Windows Registry Events

Creates key: HKLM\system\currentcontrolset\control\session manager
Creates key: HKCU\software\microsoft\windows\currentversion\run
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\1
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\2
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\3
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\4
Creates key: HKCU\software\microsoft\internet explorer\phishingfilter
Creates key: HKCU\software\microsoft\internet explorer\recovery
Creates key: HKCU\software\microsoft\systemcertificates\my
Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters
Creates key: HKCU\software\microsoft windows
Creates key: HKLM\software\wow6432node\microsoft\tracing
Creates key: HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasapi32
Creates key: HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasmancs
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\connections
Creates key: HKCU\software\appdatalow
Creates key: HKCU\software\microsoft\internet explorer\internetregistry
Creates key: HKCU\software\microsoft\internet explorer\lowregistry
Creates key: HKCU\software\microsoft\internet explorer\lowregistry\dontshowmethisdialogagain
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache
Creates key: HKCU\software\microsoft\internet explorer\intelliforms
Creates key: HKCU\software\microsoft\internet explorer\toolbar
Creates key: HKCU\software\microsoft\internet explorer\toolbar\webbrowser
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\menuorder\favorites
Creates key: HKCU\software\microsoft\internet explorer\pagesetup
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\passport\lowdamap
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\lowregistry
Creates key: HKCU\software\microsoft\internet explorer\zoom
Creates key: HKCU\software\microsoft\internet explorer\browseremulation\lowmic
Creates key: HKCU\software\microsoft\internet explorer\ietld\lowmic
Creates key: HKCU\software\microsoft\windows nt\currentversion\network\location awareness
Creates key: HKCU\software\microsoft\windows\currentversion\internet

settings\wpad\{749a4bbc-a262-40dd-a3d0-043eb10d756e}
Creates key: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{749a4bbc-a262-40dd-a3d0-043eb10d756e}\26-a0-ff-2b-56-80
Creates key: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\26-a0-ff-2b-56-80
Creates key: HKLM\software\wow6432node
Creates key: HKLM\software\wow6432node\microsoft
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: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[proxybypass]
Deletes value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap[proxybypass]
Deletes value: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[intranetname]
Deletes value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap[intranetname]
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\software\microsoft\wow64
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\spyeye_injector.exe
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\language
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings
Opens key: HKLM\software\policies\microsoft\mui\settings
Opens key: HKCU\
Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop\languageconfiguration
Opens key: HKCU\control panel\desktop
Opens key: HKCU\control panel\desktop\muicached
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key: HKLM\
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\diagnostics
Opens key: HKLM\system\currentcontrolset\control\computername
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\system\setup
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\83a49421955.exe
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\appcompat
Opens key: HKLM\software\policies\microsoft\windows\appcompat
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\83a49421955.exe
Opens key: HKLM\system\currentcontrolset\services\crypt32
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\wow6432node\microsoft\ole
Opens key: HKLM\software\wow6432node\microsoft\ole\tracing
Opens key: HKLM\software\microsoft\ole\tracing
Opens key: HKLM\software\wow6432node\microsoft\oleaut
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings

Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\w2x5c34.exe
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\w2x5c34.exe
Opens key: HKLM\software\wow6432node\microsoft\internet explorer
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\user
agent
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\user agent
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\user agent
Opens key: HKLM\software\wow6432node\policies
Opens key: HKCU\software\policies
Opens key: HKCU\software
Opens key: HKLM\software\wow6432node
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\user agent
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\user agent
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\user agent\ua tokens
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\user agent\pre platform
Opens key: HKLM\software\wow6432node\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\wow6432node\microsoft\windows\currentversion\internet
settings\user agent\post platform
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\user agent\post platform
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\post platform
Opens key: HKLM\software\wow6432node\policies\microsoft\internet
explorer\main\featurecontrol
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKLM\software\policies\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKCU\software\microsoft\windows nt\currentversion
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags
Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer
Opens key: HKLM\software\policies\microsoft\internet explorer
Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\main
Opens key: HKLM\software\policies\microsoft\internet explorer\main
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags\custom\83a49421955.exe
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 0
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov\#16
Opens key: HKLM\software\wow6432node\microsoft\rpc
Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\policies\microsoft\sqmclient\windows
Opens key: HKLM\software\wow6432node\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\software\wow6432node\microsoft\cryptography\oid\encodingtype

0\certdllopenstoreprov\ldap
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 1
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 1\certdllopenstoreprov
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\cache\content
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\explorer
Opens key: HKLM\software\policies\microsoft\windows\explorer
Opens key: HKCU\software\policies\microsoft\windows\explorer
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}\propertybag
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}\propertybag
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\profilelist\s-1-5-21-2469590586-531574596-741558139-1004
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-2469590586-531574596-741558139-1004
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\cache\cookies
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}\propertybag
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\history
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\cache\history
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}\propertybag
Opens key: HKU\
Opens key: HKCU\software\microsoft\systemcertificates\my\physicalstores
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\wow6432node\microsoft\windows\windows error reporting\wmr
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\domstore
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat
Opens key: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\extensible cache\iecompat
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016012520160201
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016020820160209
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016021220160213
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\175O6cf5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
Opens key: HKLM\software\policies\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
Opens key: HKLM\software\policies\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
Opens key: HKLM\software\policies\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\5.0\cache

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: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol\feature_allow_long_international_filenames
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_allow_long_international_filenames
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_allow_long_international_filenames
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol\feature_disallow_null_in_response_headers
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_disallow_null_in_response_headers
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_disallow_null_in_response_headers
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol\feature_digest_no_extras_in_uri
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_digest_no_extras_in_uri
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_digest_no_extras_in_uri
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
Opens key: HKLM\system\currentcontrolset\control\lsa\accessproviders
Opens key: HKLM\system\currentcontrolset\services\ldap
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\12a151be
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers
Opens key: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad
Opens key: HKLM\software\policies\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
Opens key: HKLM\software\policies\microsoft\peerdist\service
Opens key: HKLM\software\microsoft\windows nt\currentversion\peerdist\service
Opens key: HKLM\software\policies\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters
Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient
Opens key: HKLM\software\wow6432node\policies\microsoft\system\dnsclient
Opens key: HKLM\software\policies\microsoft\system\dnsclient
Opens key: HKLM\system\currentcontrolset\control\sqmservicelist
Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache
Opens key: HKLM\system\currentcontrolset\services\dns
Opens key: HKLM\software\wow6432node\policies\microsoft\windows
nt\dnsclient\dnspolicyconfig
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{fd5823ee-42c7-4e05-bbeb-
8fdd7209a8ac}
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{fd5823ee-42c7-4e05-bbeb-
8fdd7209a8ac}
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{1896ba32-049e-19e0-bea1-
806e6f6e6963}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{1896ba32-049e-19e0-bea1-
806e6f6e6963}
Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\calc.exe
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\calc.exe
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options\calc.exe
Opens key: HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasapi32
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist
Opens key: HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasmancs
Opens key: HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
Opens key: HKLM\software\microsoft\sqmclient\windows\disabledsessions\
Opens key: HKCU\software\classes\
Opens key: HKCU\software\classes\autoproxytypes
Opens key: HKCR\autoproxytypes
Opens key: HKCU\software\classes\autoproxytypes\application/x-internet-signup
Opens key: HKCR\autoproxytypes\application/x-internet-signup
Opens key: HKCU\software\classes\autoproxytypes\application/x-ns-proxy-autoconfig
Opens key: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-
68ad-4d8a-87bd-30b759fa33dd}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-
68ad-4d8a-87bd-30b759fa33dd}\propertybag
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe
Opens key: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags\custom\rundll32.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\software\policies\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
Opens key: HKLM\software\policies\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
Opens key: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
Opens key: HKLM\system\currentcontrolset\services\netbt\linkage
Opens key: HKLM\software\microsoft\com3
Opens key: HKCU\software\classes\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}
Opens key: HKCR\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}
Opens key: HKCU\software\classes\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\treatas
Opens key: HKCR\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\progid
Opens key: HKCR\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\progid
Opens key: HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}
Opens key: HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}
Opens key: HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\progid
Opens key: HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprochandler
Opens key: HKCR\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprochandler
Opens key: HKLM\software\wow6432node\microsoft\rpc\extensions
Opens key: HKLM\software\microsoft\rpc\extensions
Opens key: HKCU\software\classes\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}
Opens key: HKCR\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}
Opens key: HKCU\software\classes\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\treatas
Opens key: HKCR\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\progid
Opens key: HKCR\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\progid
Opens key: HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}
Opens key: HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}
Opens key: HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\progid
Opens key: HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprochandler
Opens key: HKCR\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprochandler
Opens key: HKLM\software\policies\microsoft\windows\windows error reporting
Opens key: HKLM\software\microsoft\windows\windows error reporting
Opens key: HKLM\software\microsoft\windows\windows error reporting\debug
Opens key: HKCU\software\microsoft\windows\windows error reporting
Opens key: HKCU\software\classes\appid\w2x5c34.exe
Opens key: HKCR\appid\w2x5c34.exe
Opens key: HKLM\software\wow6432node\microsoft\ole\appcompat
Opens key: HKLM\software\microsoft\ole\appcompat
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key:

HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider
Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
Opens key: HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
Opens key: HKLM\software\policies\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography
Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload
Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
Opens key: HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKLM\system\currentcontrolset\services\bfe
Opens key: HKCU\software\classes\wow6432node\interface\{d0074ffd-570f-4a9b-8d69-199fdba5723b}
Opens key: HKCR\wow6432node\interface\{d0074ffd-570f-4a9b-8d69-199fdba5723b}
Opens key: HKCU\software\classes\wow6432node\interface\{d0074ffd-570f-4a9b-8d69-199fdba5723b}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{d0074ffd-570f-4a9b-8d69-199fdba5723b}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}
Opens key: HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}
Opens key: HKCU\software\classes\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\treatas
Opens key: HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\progid
Opens key: HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\progid
Opens key: HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}
Opens key: HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}
Opens key: HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\progid
Opens key: HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprochandler
Opens key: HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprochandler
Opens key: HKCU\software\classes\wow6432node\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406}
Opens key: HKCR\wow6432node\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406}
Opens key: HKCU\software\classes\wow6432node\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}
Opens key: HKCR\wow6432node\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}
Opens key: HKCU\software\classes\wow6432node\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{55272a00-42cb-11ce-8135-00aa004bb851}
Opens key: HKCR\wow6432node\interface\{55272a00-42cb-11ce-8135-00aa004bb851}
Opens key: HKCU\software\classes\wow6432node\interface\{55272a00-42cb-11ce-8135-00aa004bb851}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{55272a00-42cb-11ce-8135-00aa004bb851}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
Opens key: HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
Opens key: HKCU\software\classes\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\treatas
Opens key: HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\progid
Opens key: HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\progid
Opens key: HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
Opens key: HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
Opens key: HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\progid

Opens key: HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprochandler
Opens key: HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprochandler
Opens key: HKCU\software\classes\wow6432node\interface\{bcd1de7e-2db1-418b-b047-4a74e101f8c1}
Opens key: HKCR\wow6432node\interface\{bcd1de7e-2db1-418b-b047-4a74e101f8c1}
Opens key: HKCU\software\classes\wow6432node\interface\{bcd1de7e-2db1-418b-b047-4a74e101f8c1}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{bcd1de7e-2db1-418b-b047-4a74e101f8c1}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}
Opens key: HKCR\wow6432node\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}
Opens key: HKCU\software\classes\wow6432node\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}\proxystubclsid32
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\{749a4bbc-a262-40dd-a3d0-043eb10d756e}
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\
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\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\
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\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\ranges\
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\protocoldefaults\
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\domains\
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zonemap\domains\
Opens key: HKLM\software\policies\microsoft\internet explorer\security
Opens key: HKCU\software\policies\microsoft\internet explorer
Opens key: HKCU\software\microsoft\internet explorer\security
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\security
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0

Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\0
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\1
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap\
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\2
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\4
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Opens key: HKCU\software\microsoft\windows\currentversion\internet

settings\lockdown_zones\3
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key: HKLM\software\policies\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
Opens key: HKLM\software\policies\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
Opens key: HKCU\software\microsoft\internet explorer\ietld
Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\content
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\cookies
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\history
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\00f5af79-05320ef5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\00f5af79
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\connections
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
Queries value: HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
Queries value: HKLM\software\microsoft\wow64[wow64executeflags]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]
Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
Queries value: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup[systemsetupinprogress]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
Queries value: HKCU\software\microsoft\windows
nt\currentversion\appcompatflags\layers[c:\winoldfileq\83a49421955.exe]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disablelocaloverride]
Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]

Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[83a49421955]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[disableimprovedzonecheck]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[security_hklm_only]
Queries value: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers[c:\users\admin\appdata\local\temp\w2x5c34.exe]
Queries value: HKLM\system\currentcontrolset\control\session manager[pendingfilerenameoperations2]
Queries value: HKLM\system\currentcontrolset\control\session manager[pendingfilerenameoperations]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[w2x5c34]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer[version]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[]
Queries value: HKLM\software\wow6432node\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\wow6432node\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\wow6432node\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\wow6432node\microsoft\windows\currentversion\internet settings\5.0\user agent[platform]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_browser_emulation[w2x5c34.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_browser_emulation[*]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[spyeye_injector]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[0cfe0455-93ba-440d-a3fe-553973d0b723]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[797fabac-7b58-4796-b924-d51178a59ce4]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[fromcachetimeout]
Queries value: HKLM\system\currentcontrolset\services\crypt32[diaglevel]
Queries value: HKLM\system\currentcontrolset\services\crypt32[diagmatchanymask]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[secureprotocols]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[secureprotocols]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[secureprotocols]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[certificaterevocation]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablekeepalive]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablepassport]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[idnenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[cachemode]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[enablehttp1_1]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[enablehttp1_1]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[enablehttp1_1]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[proxyhttp1.1]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[proxyhttp1.1]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyhttp1.1]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[enablenegotiate]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablebasicoverclearchannel]
Queries value: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol[feature_clientauthcertfilter]
Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol[feature_clientauthcertfilter]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol[feature_clientauthcertfilter]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[clientauthbuiltinui]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value: HKLM\software\policies\microsoft\sqmclient\windows[ceipenable]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[syncmode5]
Queries value: HKLM\software\wow6432node\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\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\cache\content[peruseritem]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[category]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[name]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[parentfolder]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[description]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[relativepath]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[parsingname]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[infotip]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[localizedname]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[icon]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[security]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresource]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresourcetype]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[localredirectonly]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[roamable]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[precreate]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[stream]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[publishexpandedpath]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[attributes]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[foldertypeid]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[cache]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[local appdata]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-

0e22-4760-9afe-ea3317b67173}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[initfolderhandler]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
2469590586-531574596-741558139-1004[profileimagepath]
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\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[streamresource]

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[cookies]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[attributes]

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[appdata]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\history[peruseritem]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\cache\history[peruseritem]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[history]
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\software\wow6432node\microsoft\windows\windows error

reporting\wmr[disable]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016012520160201[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016012520160201[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016012520160201[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016012520160201[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016012520160201[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016020820160209[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016020820160209[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016020820160209[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016020820160209[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016020820160209[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016021220160213[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016021220160213[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016021220160213[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016021220160213[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016021220160213[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]

Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[displayscriptdownloadfailureui]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[mbcsservername]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[mbcsapiforcrack]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[utf8servernameres]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
Queries value: HKLM\software\wow6432node\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\wow6432node\microsoft\windows\currentversion\internet settings[maxconnectionsperserver]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[maxconnectionsper1_0server]
Queries value: HKLM\software\wow6432node\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\wow6432node\microsoft\windows\currentversion\internet settings[connecttimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[connectretries]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[connectretries]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[sendtimeout]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[sendtimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[receivetimeout]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[receivetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablentlmpreauth]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[scavengecachelowerbound]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[certcachenovalidate]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache[scavengecachefilelifetime]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings\5.0\cache[scavengecachefilelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache[scavengecachefilelimit]
Queries value: HKLM\software\wow6432node\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\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[w2x5c34.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablecachingofsslpages]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[perusercookies]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[leashlegacycookies]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[dialupuselansettings]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[dialupuselansettings]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[sendextracrlf]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[wpadsearchalldomains]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[bypasshttpnocachecheck]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[bypasshttpnocachecheck]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[bypassssl nocachecheck]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[bypassssl nocachecheck]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[enablehttptrace]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[nocheckautodialoverride]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[nocheckautodialoverride]
Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[dontusednsloadbalancing]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
Queries value:
HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
Queries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
Queries value: HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
Queries value: HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[tcpautotuning]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad[wpadoverride]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[nonetautodial]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[badproxyexpirestime]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disablebranchcache]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\service[enable]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[w2x5c34.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[*]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache[shutdownonidle]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]

Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{fd5823ee-42c7-4e05-bbeb-8fdd7209a8ac}[searchlist]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{fd5823ee-42c7-4e05-bbeb-8fdd7209a8ac}[enabledhcp]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{fd5823ee-42c7-4e05-bbeb-8fdd7209a8ac}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{fd5823ee-42c7-4e05-bbeb-8fdd7209a8ac}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{fd5823ee-42c7-4e05-bbeb-8fdd7209a8ac}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{fd5823ee-42c7-4e05-bbeb-8fdd7209a8ac}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{fd5823ee-42c7-4e05-bbeb-8fdd7209a8ac}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{fd5823ee-42c7-4e05-bbeb-8fdd7209a8ac}[dhcpnameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{1896ba32-049e-19e0-bea1-806e6f6e6963}[enabledhcp]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{1896ba32-049e-19e0-bea1-806e6f6e6963}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{1896ba32-049e-19e0-bea1-806e6f6e6963}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{1896ba32-049e-19e0-bea1-806e6f6e6963}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{1896ba32-049e-19e0-bea1-806e6f6e6963}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{1896ba32-049e-19e0-bea1-806e6f6e6963}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{1896ba32-049e-19e0-bea1-806e6f6e6963}[dhcpnameserver]
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{fd5823ee-42c7-4e05-bbeb-8fdd7209a8ac}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{fd5823ee-42c7-4e05-bbeb-8fdd7209a8ac}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{fd5823ee-42c7-4e05-bbeb-8fdd7209a8ac}[registrationmaxaddresscount]

Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{fd5823ee-42c7-4e05-bbeb-8fdd7209a8ac}[maxnumberofaddressestoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{fd5823ee-42c7-4e05-bbeb-8fdd7209a8ac}[enablemulticast]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{1896ba32-049e-19e0-bea1-806e6f6e6963}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{1896ba32-049e-19e0-bea1-806e6f6e6963}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{1896ba32-049e-19e0-bea1-806e6f6e6963}[disabledynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{1896ba32-049e-19e0-bea1-806e6f6e6963}[enableadapterdomainnameregistration]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{1896ba32-049e-19e0-bea1-806e6f6e6963}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{1896ba32-049e-19e0-bea1-806e6f6e6963}[maxnumberofaddressestoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{1896ba32-049e-19e0-bea1-806e6f6e6963}[enablemulticast]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
Queries value: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers[c:\windows\system32\calc.exe]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
Queries value: HKLM\software\wow6432node\microsoft\tracing[enableconsoletracing]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasapi32[enablefiletracing]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasapi32[filetracingmask]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasapi32[enableconsoletracing]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasapi32[consoletracingmask]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasapi32[maxfilesize]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasapi32[filedirectory]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[programdata]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasmancs[enablefiletracing]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasmancs[filetracingmask]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasmancs[enableconsoletracing]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasmancs[consoletracingmask]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasmancs[maxfilesize]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasmancs[filedirectory]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[proxysettingsperuser]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[migrateproxy]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyenable]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyserver]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyoverride]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[autoconfigurl]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\connections[savedlegacysettings]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\connections[defaultconnectionsettings]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[autoconfigcustomua]
Queries value: HKCR\autoproxytypes\application/x-internet-signup[dllfile]
Queries value: HKCR\autoproxytypes\application/x-internet-signup[fileextensions]
Queries value: HKCR\autoproxytypes\application/x-internet-signup[default]
Queries value: HKCR\autoproxytypes\application/x-internet-signup[flags]
Queries value: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[dllfile]
Queries value: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[fileextensions]
Queries value: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[default]

Queries value: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[flags]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[favorites]
Queries value: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers[c:\windows\system32\rundll32.exe]
Queries value: HKLM\software\microsoft\windows nt\currentversion\appcompatflags[{d97b6486-0cfa-44d8-acc2-0f8b5941e889}]
Queries value: HKCU\software\microsoft\windows nt\currentversion\appcompatflags[{d97b6486-0cfa-44d8-acc2-0f8b5941e889}]
Queries value: HKLM\software\microsoft\windows nt\currentversion\appcompatflags[{44480e68-dfd5-435f-bdfe-b8246fc9f90f}]
Queries value: HKCU\software\microsoft\windows nt\currentversion\appcompatflags[{44480e68-dfd5-435f-bdfe-b8246fc9f90f}]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_mime_handling[w2x5c34.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_mime_handling[*]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip6[winsock 2.0 provider id]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]

Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
Queries value: HKLM\system\currentcontrolset\services\netbt\linkage[export]
Queries value: HKLM\software\microsoft\com3[com+enabled]
Queries value: HKCR\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}[]
Queries value: HKCR\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\ole[maxsxshashcount]
Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[werfault]
Queries value: HKCR\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}[]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[5ef9ec44-fb87-4f51-
af4e-ced084013281]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[7930f74b-e328-4350-
89c6-11fd93771488]
Queries value: HKLM\software\microsoft\windows\windows error reporting[traceflags]
Queries value: HKLM\software\microsoft\windows\windows error reporting[noreflection]
Queries value: HKCU\software\microsoft\windows\windows error reporting[noreflection]
Queries value: HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
Queries value: HKLM\software\microsoft\ole[defaultaccesspermission]
Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[type]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[image path]
Queries value: HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
Queries value: HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
Queries value: HKLM\software\microsoft\cryptography[machineguid]
Queries value: HKCR\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32[]
Queries value: HKLM\software\microsoft\rpc\extensions[remoterpcdll]
Queries value: HKLM\software\microsoft\ole[maximumallowedallocationsize]
Queries value: HKCR\wow6432node\interface\{d0074ffd-570f-4a9b-8d69-
199fdba5723b}\proxystubclsid32[]
Queries value: HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}[]
Queries value: HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32[threadingmodel]
Queries value: HKCR\wow6432node\interface\{26656eaa-54eb-4e6f-8f85-
4f0ef901a406}\proxystubclsid32[]
Queries value: HKCR\wow6432node\interface\{8a40a45d-055c-4b62-abd7-
6d613e2ceaec}\proxystubclsid32[]
Queries value: HKCR\wow6432node\interface\{55272a00-42cb-11ce-8135-
00aa004bb851}\proxystubclsid32[]
Queries value: HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}[]
Queries value: HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32[threadingmodel]
Queries value: HKCR\wow6432node\interface\{bcd1de7e-2db1-418b-b047-
4a74e101f8c1}\proxystubclsid32[]
Queries value: HKCR\wow6432node\interface\{2a1c9eb2-df62-4154-b800-
63278fcb8037}\proxystubclsid32[]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad[wpadlastnetwork]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[autoproxydetecttype]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[w2x5c34.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[*]
Queries value: HKCU\software\microsoft\internet
explorer\security[disablesecuritysettingscheck]

Queries value: HKLM\software\wow6432node\microsoft\internet explorer\security[disablesecuritysettingscheck]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[flags]
Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[w2x5c34.exe]
Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[*]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[w2x5c34.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[*]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[createuricachesize]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[createuricachesize]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[createuricachesize]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[createuricachesize]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[enablepunycode]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[enablepunycode]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[enablepunycode]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietldversionlow]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietldversionhigh]
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: HKCU\software\microsoft\windows nt\currentversion\appcompatflags[showdebuginfo]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[rundll32]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache[signature]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\content[peruseritem]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\content[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\content[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\cookies[peruseritem]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\cookies[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\cookies[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\history[peruseritem]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\history[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\history[cachelimit]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[rundll32.exe]
Sets/Creates value: HKLM\system\currentcontrolset\control\session manager[pendingfilerenameoperations]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\run[1h6wzb8fzvux1h7furzmsv]
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\0[1609]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[1406]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[1409]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet

settings\zones\2[1609]
  Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[1406]
  Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1[1406]
  Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2[1406]
  Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3[1406]
  Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4[1406]
  Sets/Creates value: HKCU\software\microsoft\internet
explorer\phishingfilter[shownservicedownballoon]
  Sets/Creates value: HKCU\software\microsoft\internet
explorer\recovery[clearbrowsinghistoryonexit]
  Sets/Creates value: HKCU\software\microsoft windows[0000003909feae51]
  Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasapi32[enablefiletracing]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasapi32[enableconsoletracing]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasapi32[filetracingmask]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasapi32[consoletracingmask]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasapi32[maxfilesize]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasapi32[filedirectory]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasmancs[enablefiletracing]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasmancs[enableconsoletracing]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasmancs[filetracingmask]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasmancs[consoletracingmask]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasmancs[maxfilesize]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\w2x5c34_rasmancs[filedirectory]
  Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{749a4bbc-a262-40dd-a3d0-043eb10d756e}[wpaddecisionreason]
  Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{749a4bbc-a262-40dd-a3d0-043eb10d756e}[wpaddecisiontime]
  Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{749a4bbc-a262-40dd-a3d0-043eb10d756e}[wpaddecision]
  Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{749a4bbc-a262-40dd-a3d0-043eb10d756e}[wpadnetworkname]
  Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\26-a0-ff-2b-56-80[wpaddecisionreason]
  Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\26-a0-ff-2b-56-80[wpaddecisiontime]
  Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\26-a0-ff-2b-56-80[wpaddecision]
  Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
  Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
  Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
  Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
  Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1409]
  Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1609]
  Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1406]
  Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1409]
  Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1609]
  Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1406]
  Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[1409]
  Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[1609]
  Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[1406]
  Value changes: HKCU\software\microsoft\internet explorer\phishingfilter[enabledv8]

Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[proxyenable]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\connections[savedlegacysettings]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\connections[defaultconnectionsettings]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\wpad[wpadlastnetwork]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[uncasintranet]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[autodetect]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[globaluseroffline]