

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 5011, Task ID: 40062

Task ID:	40062
Risk Level:	10
Date Processed:	2016-05-03 05:04:46 (UTC)
Processing Time:	62.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\spyeye_injector.exe"
Sample ID:	5011
Type:	basic
Owner:	admin
Label:	spyeye_injector.exe
Date Added:	2016-05-03 05:04:45 (UTC)
File Type:	PE32:win32:gui
File Size:	103936 bytes
MD5:	b98bb6d7428c3dbffcfcab2414c6daa2
SHA256:	fc7f54ce456c164452d8429a7fd5f52629a69338f8954e287d2664c03c37e029
Description:	None

Pattern Matching Results

10	Suspicious writeprocess: Spyeye [Banking]
10	Creates malicious mutex: Spyeye [Banking]
2	PE: Nonstandard section
6	Renames file on boot
4	Terminates process under Windows subfolder
6	Notifies system about Internet connection change
6	Modifies registry autorun entries
1	HTTP connection - response code 404 (file not found)
7	Writes to memory of system processes
5	Packer: UPX
3	Program causes a crash [Info]
5	Adds autostart object
4	Reads process memory
3	HTTP connection - response code 200 (success)
5	Abnormal sleep detected
5	PE: Contains compressed section

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\83A49421CBD.exe ["C:\WinOldFileq\83A49421CBD.exe"]
Creates process:	C:\Users\Admin\AppData\Local\Temp\CGU1EED.exe
["C:\Users\Admin\AppData\Local\Temp\CGU1EED.exe"]	
Creates process:	C:\Windows\SysWOW64\rundll132.exe ["C:\Windows\system32\rundll132.exe"
"C:\Windows\syswow64\WININET.dll",DispatchAPICall 1]	
Reads from process:	PID:340 C:\Windows\explorer.exe
Reads from process:	PID:348 C:\Windows\System32\wininit.exe
Reads from process:	PID:400 C:\Windows\System32\winlogon.exe
Reads from process:	PID:444 C:\Windows\System32\lsass.exe
Reads from process:	PID:452 C:\Windows\System32\lsm.exe
Reads from process:	PID:568 C:\Windows\System32\svchost.exe
Reads from process:	PID:636 C:\Windows\System32\svchost.exe
Reads from process:	PID:688 C:\Windows\System32\svchost.exe
Reads from process:	PID:796 C:\Windows\System32\svchost.exe
Reads from process:	PID:848 C:\Windows\System32\svchost.exe
Reads from process:	PID:952 C:\Windows\System32\svchost.exe
Reads from process:	PID:844 C:\Windows\System32\dwm.exe
Reads from process:	PID:1068 C:\Windows\System32\spoolsv.exe
Reads from process:	PID:1100 C:\Windows\System32\taskhost.exe
Reads from process:	PID:1120 C:\Windows\System32\svchost.exe
Reads from process:	PID:1188 C:\Windows\System32\svchost.exe
Reads from process:	PID:1396 C:\Windows\System32\svchost.exe
Reads from process:	PID:1804 C:\Windows\System32\UI0Detect.exe
Reads from process:	PID:1892 C:\Windows\System32\svchost.exe
Reads from process:	PID:272 C:\Windows\System32\taskhost.exe
Reads from process:	PID:1552 C:\Windows\System32\taskhost.exe
Reads from process:	PID:364 C:\Windows\System32\WinSAT.exe
Reads from process:	PID:808 C:\Windows\System32\conhost.exe
Reads from process:	PID:2112 C:\Windows\System32\mobsync.exe
Reads from process:	PID:2660 C:\Windows\System32\wbem\unsecapp.exe
Reads from process:	PID:2764 C:\Windows\System32\wbem\WmiPrvSE.exe
Reads from process:	PID:2824 C:\Windows\System32\conhost.exe

Reads from process:	PID:1644 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:1300 C:\Program Files (x86)\Adobe\Reader 9.0\Reader\reader_sl.exe
Writes to process:	PID:2916 C:\Users\Admin\AppData\Local\Temp\CGU1EED.exe
Writes to process:	PID:3036 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:1644 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2072 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:344 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2200 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2184 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2240 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2296 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2284 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2316 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2336 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2308 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2340 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2360 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2332 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2364 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2356 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2388 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2408 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2380 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2412 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2432 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2512 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2500 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2580 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2596 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2600 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2588 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2828 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2832 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2852 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:1548 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2748 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2864 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:500 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:656 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:972 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2704 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2744 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2732 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2692 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2220 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:1668 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2212 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2928 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:1860 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:1152 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:1948 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:1712 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2252 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:248 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2236 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:1740 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2420 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:1628 C:\Windows\SysWOW64\rundll32.exe
Terminates process:	C:\WinOldFile\q83A49421CBD.exe
Terminates process:	C:\Windows\Temp\spyeye_injector.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:	\BaseNamedObjects\EGg7E53Emk0ecYoUeMUM9KK13GQy9WS
Creates mutex:	\Sessions\1\BaseNamedObjects\!MSFTHISTORY!_
Creates mutex:	\Sessions\1\BaseNamedObjects\c:\users\admin!appdata!local!microsoft!windows!temporary internet files!content.ie5!
Creates mutex:	\Sessions\1\BaseNamedObjects\c:\users\admin!appdata!roaming!microsoft!windows!cookies!
Creates mutex:	\Sessions\1\BaseNamedObjects\c:\users\admin!appdata!local!microsoft!windows!history!history.ie5!
Creates mutex:	\Sessions\1\BaseNamedObjects\WininetStartupMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\WininetConnectionMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\WininetProxyRegistryMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\RasPbFile
Creates mutex:	\Sessions\1\BaseNamedObjects\ZonesCounterMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex

```

Creates mutex:      \Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex
Creates mutex:      \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex
Creates mutex:      \Sessions\1\BaseNamedObjects\!MSFTHISTORY!_LOW!_
Creates mutex:
\Sessions\1\BaseNamedObjects\c:\users\admin!appdata!local!microsoft!windows!temporary internet
files!low!content.ie5!
Creates mutex:
\Sessions\1\BaseNamedObjects\c:\users\admin!appdata!roaming!microsoft!windows!cookies!low!
Creates mutex:
\Sessions\1\BaseNamedObjects\c:\users\admin!appdata!local!microsoft!windows!history!low!history.ie5!
Creates mutex:      \Sessions\1\BaseNamedObjects\!IETld!Mutex
Creates event:       \BaseNamedObjects\SvcctrlStartEvent_A3752DX
Creates event:       \Security\LSA_AUTHENTICATION_INITIALIZED
Creates event:       \KernelObjects\SystemErrorPortReady
Creates event:       \BaseNamedObjects\BFE_Notify_Event_{a60085e8-950a-439c-a424-
c0d15d0a30bd}
Creates semaphore:   \Sessions\1\BaseNamedObjects\4FBEA4B1

```

File System Events

```

Creates:      C:\WinOldFileq
Creates:      C:\WinOldFileq\
Creates:      C:\WinOldFileq\83A49421CBD.exe
Creates:      C:\WinOldFileq\8FDC7C717274206
Creates:      C:\Users\Admin\AppData\Local\Temp\
Creates:      C:\Users\Admin\AppData\Local\Temp\CGU1EED.tmp
Creates:      C:\Users\Admin\AppData\Local\Temp\CGU1EED.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\Prefetch\SPYEYE_INJECTOR.EXE-619282B0.pf
Opens:        C:\Windows
Opens:        C:\Windows\System32\wow64.dll
Opens:        C:\Windows\System32\wow64win.dll
Opens:        C:\Windows\System32\wow64cpu.dll
Opens:        C:\Windows\system32\wow64log.dll
Opens:        C:\Windows\SysWOW64
Opens:        C:\Windows\SysWOW64\sechost.dll
Opens:        C:\Windows\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\83A49421CBD.exe
Opens:        C:\Windows\SysWOW64\apphelp.dll
Opens:        C:\Windows\AppPatch\sysmain.sdb
Opens:        C:\WinOldFileq\ui\SwDRM.dll
Opens:        C:\Windows\Prefetch\83A49421CBD.EXE-8B5C1E36.pf
Opens:        C:\Windows\SysWOW64\imm32.dll
Opens:        C:\WinOldFileq\MSIMG32.dll
Opens:        C:\Windows\SysWOW64\msimg32.dll
Opens:        C:\WinOldFileq\8FDC7C717274206
Opens:        C:\Users\Admin\AppData\Local\Temp
Opens:        C:\Users\Admin\AppData\Local\Temp\CGU1EED.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:\Windows\Prefetch\CGU1EED.EXE-9423C11C.pf
Opens:        C:\Users\Admin\AppData\Local\Temp\MSIMG32.dll
Opens:        C:\windows\temp\spyeye_injector.exe
Opens:        C:\Program Files (x86)\Adobe\Reader 9.0\Reader\MSIMG32.dll
Opens:        C:\Windows\SysWOW64\wininet.dll
Opens:        C:\Users\Admin\AppData\Local\Temp\USERENV.dll
Opens:        C:\Windows\SysWOW64\userenv.dll
Opens:        C:\Users\Admin\AppData\Local\Temp\profapi.dll
Opens:        C:\Windows\SysWOW64\profapi.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\user32.dll
Opens:        C:\Windows\SysWOW64\ws2_32.dll

```

Opens: C:\Windows\SysWOW64\advapi32.dll
 Opens: C:\Windows\SysWOW64\crypt32.dll
 Opens: C:\Windows\SysWOW64\tzres.dll
 Opens: C:\Windows\SysWOW64\en-US\tzres.dll.mui
 Opens: C:\Users\Admin\AppData\Local\Temp\CGU1EED.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\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:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Files\Content.IE5\index.dat
 Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
 Opens:
 C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
 Opens: C:\Windows\SysWOW64\mswsock.dll
 Opens: C:\Windows\SysWOW64\WSHTCPIP.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:\Users\Admin\AppData\Local\Temp\WINNSI.DLL
 Opens: C:\Windows\SysWOW64\winnsi.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\nlaapi.dll
 Opens: C:\Windows\Prefetch\RUNDLL32.EXE-87432CEE.pf
 Opens: C:\Users\Admin\AppData\Local\Temp\rasadhlp.dll
 Opens: C:\Windows\SysWOW64\rasadhlp.dll
 Opens: C:\Windows\Prefetch\WERFAULT.EXE-37549B7E.pf
 Opens: C:\Windows\SysWOW64\psapi.dll
 Opens: C:\Windows\AppPatch\AcLayers.dll
 Opens: C:\Windows\SysWOW64\winpool.drv
 Opens: C:\Windows\SysWOW64\mpr.dll
 Opens: C:\Windows\AppPatch\acwow64.dll
 Opens: C:\Windows\SysWOW64\version.dll
 Opens: C:\Windows\SysWOW64\en-US\rundll32.exe.mui
 Opens: C:\Windows\SysWOW64\WININET.dll.manifest
 Opens: C:\Windows\SysWOW64\uxtheme.dll
 Opens: C:\Windows\SysWOW64\dwmapapi.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
Opens: C:\Windows\SysWOW64\NapiNSP.dll
Opens: C:\Windows\SysWOW64\pnprnsp.dll
Opens: C:\Windows\SysWOW64\winrnr.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:\Users\Admin\AppData\Local\Temp\ntmarta.dll
Opens: C:\Windows\SysWOW64\ntmarta.dll
Opens: C:\Users\Admin\AppData\Local\Temp\VERSION.dll
Opens: C:\Windows\SysWOW64\en-US\urlmon.dll.mui
Opens: C:\Windows\SysWOW64\wship6.dll
Opens: C:\Windows\SysWOW64\FWPuclnt.DLL
Writes to: C:\WinOldFileq\83A49421CBD.exe
Writes to: C:\WinOldFileq\8FDC7C717274206
Writes to: C:\Users\Admin\AppData\Local\Temp\CGU1EED.exe
Reads from: C:\Windows\SysWOW64\ntdll.dll
Reads from: C:\Windows\Temp\spyeye_injector.exe
Reads from: C:\WinOldFileq\83A49421CBD.exe
Reads from: C:\WinOldFileq\8FDC7C717274206
Reads from: C:\Users\Admin\AppData\Local\Temp\CGU1EED.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\SysWOW64\rundll32.exe
Reads from: C:\Windows\System32\drivers\etc\hosts
Deletes: C:\Windows\Temp\spyeye_injector.exe

Network Events

DNS query:	alexeyartemov.com
DNS query:	www.microsoft.com
DNS response:	alexeyartemov.com ⇒ 198.105.244.11
DNS response:	alexeyartemov.com ⇒ 104.239.213.7
DNS response:	e10088.dspb.akamaiedge.net ⇒ 96.6.72.154
DNS response:	e10088.dspb.akamaiedge.net ⇒ 104.109.84.116
Connects to:	88.198.13.147:443
Connects to:	8.8.8.8:53
Connects to:	4.2.2.1:53
Connects to:	198.105.244.11:80
Connects to:	104.239.213.7:80
Connects to:	96.6.72.154:80
Sends data to:	8.8.8.8:53
Sends data to:	4.2.2.1:53
Sends data to:	88.198.13.147:443
Sends data to:	alexeyartemov.com:80 (198.105.244.11)
Sends data to:	alexeyartemov.com:80 (104.239.213.7)
Sends data to:	e10088.dspb.akamaiedge.net:80 (96.6.72.154)
Receives data from:	8.8.8.8:53
Receives data from:	4.2.2.1:53
Receives data from:	88.198.13.147:443
Receives data from:	alexeyartemov.com:80 (198.105.244.11)
Receives data from:	alexeyartemov.com:80 (104.239.213.7)
Receives data from:	e10088.dspb.akamaiedge.net:80 (96.6.72.154)

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: HKCU\software\microsoft windows

Creates key: HKLM\software\wow6432node\microsoft\tracing

Creates key: HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32

Creates key: HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasmancs

Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\connections

Creates key: HKCU\software\apdata\low

Creates key: HKCU\software\microsoft\internet explorer\internetregistry

Creates key: HKCU\software\microsoft\internet explorer\lowregistry

Creates key: HKCU\software\microsoft\internet explorer\lowregistry\dontshowmethisdialogagain

Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache

Creates key: HKCU\software\microsoft\internet explorer\intelliforms

Creates key: HKCU\software\microsoft\internet explorer\toolbar

Creates key: HKCU\software\microsoft\internet explorer\toolbar\webbrowser

Creates key: HKCU\software\microsoft\windows\currentversion\explorer\menuorder\favorites

Creates key: HKCU\software\microsoft\internet explorer\pagesetup

Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\passport\lowdamap

Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad

Creates key: HKCU\software\microsoft\windows\currentversion\explorer\lowregistry

Creates key: HKCU\software\microsoft\internet explorer\zoom

Creates key: HKCU\software\microsoft\internet explorer\browseremulation\lowmic

Creates key: HKCU\software\microsoft\internet explorer\ietld\lowmic

Creates key: HKCU\software\microsoft\windows nt\currentversion\network\location awareness

Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters

Creates key: HKLM\software\wow6432node

Creates key: HKLM\software\wow6432node\microsoft

Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\p3p\history

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\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\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\83a49421cbd.exe
 Opens key: HKLM\system\currentcontrolset\control\session manager\apccertdlls
 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\83a49421cbd.exe
 Opens key: HKLM\system\currentcontrolset\services\crypt32
 Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
 execution options\83a49421cbd.exe
 Opens key: HKCU\software\microsoft\windows nt\currentversion
 Opens key: HKLM\software\wow6432node\microsoft\windows
 nt\currentversion\appcompatflags
 Opens key: HKLM\software\wow6432node\microsoft\windows
 nt\currentversion\appcompatflags\custom\83a49421cbd.exe
 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\cgu1eed.exe
 Opens key: HKLM\software\microsoft\windows
 nt\currentversion\appcompatflags\custom\cgu1eed.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: 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\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\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: HKU\
Opens key: HKCU\software\microsoft\systemcertificates\my\physicalstores
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
980053277-1733835069-2361817685-1001
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\system\currentcontrolset\control\cmf\config
Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
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\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\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\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\currentversion\explorer\knownfolderssettings

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: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache

Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore

Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat

Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat

Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld

Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:

Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset

Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset

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: 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: 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: 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: 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: 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: 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\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\17506cf5
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: 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\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
Opens key: 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: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
Opens key: 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\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
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\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\appid_catalog\1b6e5dd2
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters

Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
 Opens key: HKLM\system\currentcontrolset\services\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: 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: 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\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32
 Opens key: HKLM\software\wow6432node\microsoft\windows
 nt\currentversion\profilelist
 Opens key: HKLM\software\microsoft\sqlclient\windows\disabledprocesses\
 Opens key: HKLM\software\microsoft\sqlclient\windows\disabledsessions\
 Opens key: HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasmancs
 Opens key: HKLM\system\currentcontrolset\control\sqlmservicelist
 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: 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: 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\dnsclient\parameters
 Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
 Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient
 Opens key: HKLM\system\currentcontrolset\services\dns
 Opens key: HKLM\software\wow6432node\policies\microsoft\windows
 nt\dnsclient\dnsclientpolicyconfig
 Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient\dnsclientpolicyconfig
 Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient\dnsclientpolicyconfig
 Opens key: HKLM\system\currentcontrolset\services\dnsclient\parameters\dnsclientpolicyconfig
 Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\
 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: 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

[illegible]

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: HKLM\software\wow6432node\microsoft\windows nt\currentversion\aebug
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solids_in_userinfo_kb932562
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solids_in_userinfo_kb932562
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: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\feedplat
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\iecompat
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\ietld
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\privacie:
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
Opens key: HKLM\software\wow6432node\policies\microsoft\system\dnsclient
Opens key: HKLM\software\policies\microsoft\system\dnsclient
Opens key: HKLM\system\currentcontrolset\services\dnsclient\parameters\dnsclient
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a91d0a5e-390e-4979-9c38-127795c4e47a}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b9ec5865-2d36-4cb8-b474-65fee5bae0b1}

Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage
 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: HKLM\system\currentcontrolset\control\lsa\accessproviders
 Opens key: HKLM\system\currentcontrolset\services\ldap
 Opens key: HKCU\software\microsoft\internet explorer\ietld
 Opens key: HKLM\system\currentcontrolset\services\winsock\setup
 migration\providers\tcpip6
 Opens key: HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_zone_elevation
 Opens key: HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_zone_elevation
 Opens key: HKCU\software\microsoft\windows\currentversion\internet
 settings\p3p\history\microsoft.com
 Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options[disableusermodecallbackfilter]
 Queries value: HKLM\system\currentcontrolset\control\session
 manager[cwdillegalindllsearch]
 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
 Queries value:
 HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
 Queries value: HKLM\system\currentcontrolset\control\locale\customlocale[empty]
 Queries value:
 HKLM\system\currentcontrolset\control\locale\language[installlanguagefallback]
 Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
 Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-
 us[alternatencodepage]
 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\locale\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\locale\customlocale[en-us]
 Queries value: HKLM\system\currentcontrolset\control\locale\extendedlocale[en-us]
 Queries value:
 HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticcodeenabled]
 Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell
 folders[cache]
 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[83a49421cbd]
 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[pageallocatorssystemheapisprivate]
 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: 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[cgufeed]
 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[cgufeed.exe]
  Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation[*]
  Queries value: HKLM\system\currentcontrolset\services\crypt32[diaglevel]
  Queries value: HKLM\system\currentcontrolset\services\crypt32[diagmatchanymask]
  Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
980053277-1733835069-2361817685-1001[profileimagepath]
  Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
  Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
  Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
  Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
  Queries value: 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[disablebasiccoverclearchannel]
  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\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}[parent folder]
  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}[parsiname]
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: 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[cache\limit]
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}[parsiname]
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}[parsiname]
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}[parsiname]
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: 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[cacheopath]
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[cacheopath]
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[cacheopath]
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[cacheopath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]

Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[displayscriptdownloadfailureui]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsservername]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsapiforcrack]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[utf8servernameses]
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\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
Queries value: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[cgu1eed.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
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: 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:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
Queries value: 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[bypasssslnocachecheck]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings[bypasssslnocachecheck]
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\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:

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[storiesserviceclassinfo]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
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:
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: HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscheenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscheentries]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnschetimeout]
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:
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[storserviceclassinfo]
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: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[tcpautotuning]
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[storserviceclassinfo]
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[storserviceclassinfo]
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[storiesserviceclassinfo]
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[storiesserviceclassinfo]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\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[badproxyexpiretime]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings[disablebranchcache]
Queries value: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_http_username_password_disable[cgu1eed.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_http_username_password_disable[*]
Queries value: HKLM\software\wow6432node\microsoft\tracing[enableconsoletracing]
Queries value:

HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[enablefiletracing]
Queries value:

HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[filetracingmask]
Queries value:

HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[enableconsoletracing]
Queries value:

HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[consoletracingmask]
Queries value:

HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[maxfilesize]
Queries value:

HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[filedirectory]
Queries value: HKLM\software\microsoft\windows

nt\currentversion\profilelist[programdata]
Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[dd79cc82]

Queries value:
HKLM\software\microsoft\sqlclient\windows\disabledsessions[machinethrottling]
Queries value:
HKLM\software\microsoft\sqlclient\windows\disabledsessions[globalsession]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasmancs[enablefiletracing]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasmancs[filetracingmask]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasmancs[enableconsoletracing]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasmancs[consoletracingmask]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasmancs[maxfilesize]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasmancs[filedirectory]
Queries value: HKLM\system\currentcontrolset\control\sqlservicelist[sqlservicelist]
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:
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}[streamresourcecetype]
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: 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[cgufeed.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[*]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodiald11]
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[screndefaultservers]
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[usedns]
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[maxnumberofaddresstoregister]
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[adapertimeoutlimit]
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\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[cguleed.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[*]
Queries value: HKLM\software\policies\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[cguleed.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[cgu1eed.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\aedebug[debugger]
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\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: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\feedplat[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\feedplat[cacheopath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\feedplat[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\feedplat[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\feedplat[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\iecompat[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\iecompat[cacheopath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\iecompat[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\iecompat[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\iecompat[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\ietld[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\ietld[cacheopath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\ietld[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\ietld[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\ietld[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\privacie:[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\privacie:[cacheopath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\lowcache\extensible cache\privacie:[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\privacie:[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\privacie:[cacheoptions]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[rundll32.exe]
Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a66e19e6]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters\dnsCache[shutdownonidle]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[searchlist]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[enabledhcp]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[dhcpv6domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[dhcpnameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[enabledhcp]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpnameserver]
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[maxnumberofaddressesstoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[enablemulticast]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[queryadaptername]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[disablenameregistration]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[enablemulticast]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[maxnumberofaddressesstoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[searchlist]
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[usehostnamesasaliases]
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]
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\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation[cgu1eed.exe]
Queries value:
HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation[*]
Queries value:
HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[{aeba21fa-782a-4a90-978d-b72164c80120}]
Queries value:
HKCU\software\microsoft\windows\currentversion\internet settings[privacyadvanced]
Sets/Creates value: HKLM\system\currentcontrolset\control\session manager[pendingfilerenameoperations]
Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\run[1h6wzb8fyvuwzwwulyaty]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[1409]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[1609]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[1406]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\1[1406]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\2[1406]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\3[1406]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\4[1406]
Sets/Creates value: HKCU\software\microsoft\internet explorer\phishingfilter[shownservicedownballoon]
Sets/Creates value: HKCU\software\microsoft\internet explorer\recovery[clearbrowsinghistoryonexit]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings[globaluseroffline]
Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[enablefiletracing]
Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[enableconsoletracing]
Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[filetracingmask]
Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[consoletracingmask]
Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[maxfilesize]
Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[filedirectory]
Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasmancs[enablefiletracing]

Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasmancs[enableconsoletracing]
Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasmancs[filetracingmask]
Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasmancs[consoletracingmask]
Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasmancs[maxfilesize]
Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasmancs[filedirectory]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonintranet]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1409]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1609]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1406]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[1409]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[1609]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[1406]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1409]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1609]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1406]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[1409]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[1609]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[1406]
Value changes: HKCU\software\microsoft\internet explorer\phishingfilter[enabledv8]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[uncasintranet]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]