

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

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

| | |
|----------------------|--|
| Task ID: | 1 |
| Risk Level: | 10 |
| Date Processed: | 2016-03-28 07:35:09 (UTC) |
| Processing Time: | 63.49 seconds |
| Virtual Environment: | IntelliVM |
| Execution Arguments: | "c:\windows\temp\spyeye_injector.exe" |
| Sample ID: | 1 |
| Type: | basic |
| Owner: | admin |
| Label: | spyeye_injector.exe |
| Date Added: | 2016-03-28 07:35:09 (UTC) |
| File Type: | PE32:win32:gui |
| File Size: | 103936 bytes |
| MD5: | b98bb6d7428c3dbffcfcab2414c6daa2 |
| SHA256: | fc7f54ce456c164452d8429a7fd5f52629a69338f8954e287d2664c03c37e029 |
| Description: | None |

Pattern Matching Results

| | |
|----|---|
| 7 | Writes to memory of system processes |
| 6 | Modifies registry autorun entries |
| 10 | Suspicious writeprocess: Spyeye [Banking] |
| 5 | Abnormal sleep detected |
| 3 | Connects to local host |
| 2 | PE: Nonstandard section |
| 4 | Reads process memory |
| 5 | PE: Contains compressed section |
| 6 | Renames file on boot |
| 5 | Packer: UPX |
| 5 | Adds autostart object |
| 10 | Creates malicious mutex: Spyeye [Banking] |

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\83A49421850.exe ["C:\WinOldFileq\83A49421850.exe"] |
| Creates process: | C:\Users\Admin\AppData\Local\Temp\3MU581D.exe |
| ["C:\Users\Admin\AppData\Local\Temp\3MU581D.exe"] | |
| Reads from process: | PID:1100 C:\Windows\explorer.exe |
| Reads from process: | PID:408 C:\Windows\System32\wininit.exe |
| Reads from process: | PID:480 C:\Windows\System32\lsass.exe |
| Reads from process: | PID:488 C:\Windows\System32\winlogon.exe |
| Reads from process: | PID:592 C:\Windows\System32\svchost.exe |
| Reads from process: | PID:624 C:\Windows\System32\svchost.exe |
| Reads from process: | PID:708 C:\Windows\System32\svchost.exe |
| Reads from process: | PID:716 C:\Windows\System32\dwm.exe |
| Reads from process: | PID:788 C:\Windows\System32\svchost.exe |
| Reads from process: | PID:852 C:\Windows\System32\svchost.exe |
| Reads from process: | PID:888 C:\Windows\System32\svchost.exe |
| Reads from process: | PID:312 C:\Windows\System32\spoolsv.exe |
| Reads from process: | PID:552 C:\Windows\System32\svchost.exe |
| Reads from process: | PID:664 C:\Windows\System32\svchost.exe |
| Reads from process: | PID:1424 C:\Windows\System32\svchost.exe |
| Reads from process: | PID:2020 C:\Windows\System32\taskhost.exe |
| Reads from process: | PID:1220 C:\Windows\System32\dlh.exe |
| Reads from process: | PID:2060 C:\Windows\System32\svchost.exe |
| Reads from process: | PID:1928 C:\Windows\System32\wbem\unsecapp.exe |
| Reads from process: | PID:1840 C:\Windows\System32\wbem\WmiPrvSE.exe |
| Reads from process: | PID:2896 C:\Windows\System32\conhost.exe |
| Writes to process: | PID:2416 C:\Program Files (x86)\Adobe\Reader 9.0\Reader\reader_sl.exe |
| Writes to process: | PID:2936 C:\Users\Admin\AppData\Local\Temp\3MU581D.exe |
| Writes to process: | PID:2912 C:\Windows\Temp\spyeye_injector.exe |
| Writes to process: | PID:2896 C:\Windows\System32\conhost.exe |
| Terminates process: | C:\WinOldFileq\83A49421850.exe |
| Terminates process: | C:\Windows\Temp\spyeye_injector.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\055a1WUoIYACUYKgMCIWOEMUQISIQ
Creates mutex: \Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex
Creates mutex: \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex
Creates semaphore: \Sessions\1\BaseNamedObjects\4FBEA4B1

File System Events

Creates: C:\WinOldFileq
Creates: C:\WinOldFileq\
Creates: C:\WinOldFileq\83A49421850.exe
Creates: C:\WinOldFileq\6C3E79A93CD5139
Creates: C:\Users\Admin\AppData\Local\Temp\
Creates: C:\Users\Admin\AppData\Local\Temp\3MU581D.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\3MU581D.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
Opens: C:\Windows\Prefetch\SPYEYE_INJECTOR.EXE-619282B0.pf
Opens: C:\Windows
Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\SysWOW64
Opens: C:\Windows\SysWOW64\apphelp.dll
Opens: C:\Windows\Temp\spyeye_injector.exe
Opens: C:\Windows\SysWOW64\ntdll.dll
Opens: C:\Windows\SysWOW64\kernel32.dll
Opens: C:\Windows\SysWOW64\KernelBase.dll
Opens: C:\Windows\apppatch\sysmain.sdb
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\Windows\SysWOW64\msvcrt.dll
Opens: C:\Windows\SysWOW64\bcryptprimitives.dll
Opens: C:\Windows\SysWOW64\cryptbase.dll
Opens: C:\Windows\SysWOW64\sspicli.dll
Opens: C:\Windows\SysWOW64\rpcrt4.dll
Opens: C:\Windows\SysWOW64\advapi32.dll
Opens: C:\
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\WinOldFileq
Opens: C:\WinOldFileq\
Opens: C:\WinOldFileq\83A49421850.exe
Opens: C:\Windows\Prefetch\83A49421850.EXE-56DEA472.pf
Opens: C:\Windows\SysWOW64\msasn1.dll
Opens: C:\Windows\SysWOW64\crypt32.dll
Opens: C:\Windows\SysWOW64\ntsi.dll
Opens: C:\Windows\SysWOW64\ws2_32.dll
Opens: C:\Windows\SysWOW64\iertutil.dll
Opens: C:\Windows\SysWOW64\wininet.dll
Opens: C:\Windows\SysWOW64\gdi32.dll
Opens: C:\Windows\SysWOW64\user32.dll
Opens: C:\Windows\SysWOW64\shlwapi.dll
Opens: C:\Windows\SysWOW64\imm32.dll
Opens: C:\Windows\SysWOW64\msctf.dll
Opens: C:\Windows\SysWOW64\msimg32.dll
Opens: C:\Windows\SysWOW64\combase.dll
Opens: C:\Windows\SysWOW64\ole32.dll
Opens: C:\Windows\SysWOW64\urlmon.dll
Opens: C:\Windows\SysWOW64\oleaut32.dll
Opens: C:\Windows\SysWOW64\shell32.dll
Opens: C:\WinOldFileq\6C3E79A93CD5139
Opens: C:\Users\Admin\AppData\Local\Temp\3MU581D.exe
Opens: C:\Users\Admin\AppData\Local\Temp
Opens: C:\Users
Opens: C:\Users\Admin
Opens: C:\Users\Admin\AppData
Opens: C:\Users\Admin\AppData\Local
Opens: C:\Windows\Prefetch\3MU581D.EXE-B9DB56B9.pf
Opens: C:\Windows\SysWOW64\SHCore.dll
Opens: C:\Windows\SysWOW64\uxtheme.dll
Opens: C:\Windows\SysWOW64\profapi.dll
Opens: C:\Windows\SysWOW64\secur32.dll
Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\AppDataContainerUserCertRead
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:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\counters.dat
Opens: C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985
Opens: C:\Windows\WinSxS\x86_microsoft.windows.common-

controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll

Opens: C:\Windows\WindowsShell.Manifest
Opens: C:\Windows\SysWOW64\tzres.dll
Opens: C:\Windows\SysWOW64\en-US\tzres.dll.mui
Opens: C:\Windows\SysWOW64\winhttp.dll
Opens: C:\Windows\SysWOW64\mswsock.dll
Opens: C:\Windows\SysWOW64\IPHLPAPI.DLL
Opens: C:\Windows\SysWOW64\winnsi.dll
Opens: C:\Windows\SysWOW64\clbcatq.dll
Opens: C:\Windows\SysWOW64\cryptsp.dll
Opens: C:\Windows\SysWOW64\rsaenh.dll
Opens: C:\Windows\SysWOW64\dnsapi.dll
Opens: C:\Windows\SysWOW64\netapi32.dll
Opens: C:\Windows\SysWOW64\netutils.dll
Opens: C:\Windows\SysWOW64\srvccli.dll
Opens: C:\Windows\SysWOW64\wksccli.dll
Opens: C:\Windows\SysWOW64\nlaapi.dll
Opens: C:\Windows\SysWOW64\rasadhlp.dll
Opens: C:\Windows\SysWOW64\FWPUCFLT.DLL
Opens: C:\Windows\SysWOW64\NapiNSP.dll
Opens: C:\Windows\SysWOW64\pnrpnp.dll
Opens: C:\Windows\SysWOW64\winrnr.dll
Opens: C:\Windows\SysWOW64\dhcpcsvc6.dll
Opens: C:\Windows\SysWOW64\dhcpcsvc.dll
Opens: C:\Windows\System32\Drivers\etc\hosts
Writes to: C:\WinOldFileq\83A49421850.exe
Writes to: C:\WinOldFileq\6C3E79A93CD5139
Writes to: C:\Users\Admin\AppData\Local\Temp\3MU581D.exe
Reads from: C:\Windows\SysWOW64\ntdll.dll
Reads from: C:\Windows\Temp\spyeye_injector.exe
Reads from: C:\WinOldFileq\83A49421850.exe
Reads from: C:\WinOldFileq\6C3E79A93CD5139
Reads from: C:\Users\Admin\AppData\Local\Temp\3MU581D.exe
Reads from: C:\Windows\SysWOW64\user32.dll
Reads from: C:\Windows\SysWOW64\wininet.dll
Reads from: C:\Windows\SysWOW64\ws2_32.dll
Reads from: C:\Windows\SysWOW64\advapi32.dll
Reads from: C:\Windows\SysWOW64\crypt32.dll
Reads from: C:\Windows\System32\Drivers\etc\hosts
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 ⇒ 23.7.35.22 |
| DNS response: | e10088.dspb.akamaiedge.net ⇒ 184.86.231.62 |
| DNS response: | e10088.dspb.akamaiedge.net ⇒ 23.72.44.137 |
| DNS response: | e10088.dspb.akamaiedge.net ⇒ 23.221.32.209 |
| DNS response: | e10088.dspb.akamaiedge.net ⇒ 23.46.28.174 |
| Connects to: | 88.198.13.147:443 |
| Connects to: | 198.105.244.11:80 |
| Connects to: | 0.0.0.0:80 |
| Connects to: | 127.0.0.1:80 |
| Connects to: | 104.239.213.7:80 |
| 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: | 0.0.0.0:53 |
| Receives data from: | 8.8.8.8:53 |
| Receives data from: | 4.2.2.1:53 |
| Receives data from: | alexeyartemov.com:80 (198.105.244.11) |
| Receives data from: | 0.0.0.0:53 |

Windows Registry Events

| | |
|---------------------------|---|
| Creates key: | HKLM\system\currentcontrolset\control\session manager |
| Creates key: | HKCU\software\microsoft\windows\currentversion\run |
| Creates key: | HKCU\software\microsoft\windows\currentversion\internet settings |
| Creates key: | HKCU\software\microsoft\windows\currentversion\internet settings\zones\0 |
| Creates key: | HKCU\software\microsoft\windows\currentversion\internet settings\zones\1 |
| Creates key: | HKCU\software\microsoft\windows\currentversion\internet settings\zones\2 |
| Creates key: | HKCU\software\microsoft\windows\currentversion\internet settings\zones\3 |
| Creates key: | HKCU\software\microsoft\windows\currentversion\internet settings\zones\4 |
| settings\lockdown_zones\1 | |
| 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 |

```

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: HKCU\software\microsoft\windows\currentversion\internet
settings\connections
  Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters
  Creates key: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
  Creates key: HKCU\software\microsoft\windows nt\currentversion\network\location
awareness
  Creates key: HKCU\software
  Creates key: HKCU\software\microsoft
  Creates key: HKCU\software\microsoft\windows nt
  Creates key: HKCU\software\microsoft\windows nt\currentversion
  Creates key: HKCU\software\microsoft\windows nt\currentversion\network
  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[autodetect]
  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\wow64
  Opens key: HKLM\system\currentcontrolset\control\terminal server
  Opens key: HKLM\system\currentcontrolset\control\safeboot\option
  Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
  Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key: HKLM\system\currentcontrolset\control\nls\language
  Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages
  Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
  Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
  Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings
  Opens key: HKLM\software\policies\microsoft\mui\settings
  Opens key: HKCU\
  Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
  Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
  Opens key: HKCU\software\policies\microsoft\control panel\desktop
  Opens key: HKCU\control panel\desktop\languageconfiguration
  Opens key: HKCU\control panel\desktop
  Opens key: HKCU\control panel\desktop\muicached
  Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
  Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
  Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
  Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
  Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation
  Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
  Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dlloptions
  Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
  Opens key: HKLM\system\currentcontrolset\control\lsa
  Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
  Opens key: HKLM\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\system\currentcontrolset\control\nls\sorting\ids
  Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\83a49421850.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\83a49421850.exe
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\
Opens key: HKLM\system\currentcontrolset\services\crypt32
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\wow6432node\microsoft\ole
Opens key: HKLM\software\wow6432node\microsoft\ole\tracing
Opens key: HKLM\software\microsoft\ole\tracing
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\3mu581d.exe
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\3mu581d.exe
Opens key: HKLM\software\wow6432node\microsoft\internet explorer
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\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: 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\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\policies\microsoft\sqlclient\windows
Opens key: HKLM\software\microsoft\sqlclient\windows
Opens key: HKLM\software\wow6432node\microsoft\windows\tablet pc\
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\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\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-1-5-21-1923240461-1905901954-2556564120-1001
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1923240461-1905901954-2556564120-1001
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\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache
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: HKU\default
Opens key: HKU\default\software\microsoft\windows\currentversion\explorer\user
shell folders
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
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: 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_mime_handling
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy
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_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: 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_allow_long_international_filenames
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
Opens key: HKLM\software\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: 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\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\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
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_preserve_spaces_in_filenames_kb952730
Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_preserve_spaces_in_filenames_kb952730
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings

Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer

Opens key: HKLM\software\policies\microsoft\internet explorer

Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\main

Opens key: HKLM\software\policies\microsoft\internet explorer\main

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings
Opens key: HKLM\system\currentcontrolset\control\cmf\config

Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr

Opens key: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache
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_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_sch_send_aux_record_kb_2618444
Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_sch_send_aux_record_kb_2618444
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\2e7a8a54

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\winsock\setup_migration\providers
Opens key: HKLM\system\currentcontrolset\services\winsock\setup_migration\providers\tcpip
Opens key: HKLM\software\policies\microsoft\peerdist\service
Opens key: HKLM\software\microsoft\windows nt\currentversion\peerdist\service
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\winsock\setup_migration\providers\tcpip6
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content
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\knownfoldersettings
Opens key: HKCU\software\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\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: HKLM\software\wow6432node\microsoft\rpc\extensions
Opens key: HKLM\software\microsoft\rpc\extensions
Opens key: HKCU\software\classes\
Opens key: HKLM\software\microsoft\com3
Opens key: HKLM\software\microsoft\windowsruntime\clsid
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{00000323-0000-0000-c000-000000000046}
Opens key: HKCR\activatableclasses\clsid
Opens key: HKCR\activatableclasses\clsid\{00000323-0000-0000-c000-000000000046}
Opens key: HKLM\software\wow6432node\microsoft\oleaut
Opens key: HKCU\software\classes\wow6432node\clsid\{00000323-0000-0000-c000-000000000046}
Opens key: HKCR\wow6432node\clsid\{00000323-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\clsid\{00000323-0000-0000-c000-000000000046}
Opens key: HKCR\clsid\{00000323-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\activatableclasses\clsid
Opens key: HKCU\software\classes\activatableclasses\clsid\{00000323-0000-0000-c000-

000000000046}
Opens key: HKCU\software\classes\appid\3mu581d.exe
Opens key: HKCR\appid\3mu581d.exe
Opens key: HKLM\software\wow6432node\microsoft\ole\appcompat
Opens key: HKLM\software\microsoft\ole\appcompat
Opens key:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider
Opens key: HKLM\software\policies\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography
Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload
Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
000000000046}
Opens key: HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
000000000046}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{a168aad-1674-49da-ad4f-4f27df8760d0}
Opens key: HKCR\wow6432node\interface\{a168aad-1674-49da-ad4f-4f27df8760d0}
Opens key: HKCU\software\classes\wow6432node\interface\{a168aad-1674-49da-ad4f-4f27df8760d0}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{a168aad-1674-49da-ad4f-4f27df8760d0}\proxystubclsid32
000000000046}\proxystubclsid32
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}
60ce2149e33c}
Opens key: HKCR\activatableclasses\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}
Opens key: HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}
60ce2149e33c}
Opens key: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}
Opens key: HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\treatas
Opens key: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprocserver32
60ce2149e33c}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprochandler32
60ce2149e33c}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprochandler
Opens key: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprochandler
60ce2149e33c}\inprochandler
Opens key: HKLM\system\currentcontrolset\control\sqmservicelist
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\dnsclient\dnspolicyconfig
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient\dnsclient\dnspolicyconfig
Opens key:
HKLM\system\currentcontrolset\services\dnsclient\parameters\dnspolicyconfig
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\winhttp
Opens key: HKLM\system\currentcontrolset\services\winhttp\autoproxy\parameters
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\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\zonemap\ranges\
Opens key: HKCU\zonemap\ranges\
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 settings\zonemap
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet

[illegible]

settings\lockdown_zones\1
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
Opens key: HKLM\system\currentcontrolset\services\lanmanworkstation\parameters
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: HKLM\software\wow6432node\policies\microsoft\system\dnsclient
Opens key: HKLM\software\policies\microsoft\system\dnsclient
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a04231f6-42eb-4732-b850-25b8d56dd1d8}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4defd920-8095-41dc-aef5-8a6dc56e0da9}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}
Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage
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[transparentenables]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]
Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
Queries value: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value: HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dlloptions[usefilter]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dlloptions[spyeye_injector.exe]
Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
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\system\currentcontrolset\control\locale\sorting\versions[000602xx]
Queries value: HKLM\system\currentcontrolset\control\locale\sorting\ids[en-us]
Queries value: HKLM\system\currentcontrolset\control\locale\sorting\ids[en]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticcodeenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cache]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dlloptions[83a49421850.exe]
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[83a49421850]
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\microsoft\ole[aggressivemtestesting]
Queries value: HKLM\system\currentcontrolset\control\session manager[pendingfilerenameoperations2]
Queries value: HKLM\system\currentcontrolset\control\session manager[pendingfilerenameoperations]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dlloptions[3mu581d.exe]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[3mu581d]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer[version]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[security_hklm_only]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_browser_emulation[3mu581d.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_browser_emulation[*]
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: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[spyeye_injector]
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\5.0\user agent[platform]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\user agent[platform]
Queries value: HKLM\software\microsoft\sqlclient\windows[ceipenable]
Queries value: HKLM\software\wow6432node\microsoft\windows\tablet pc[istabletpc]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value: HKLM\software\microsoft\rpc[idletimerwindow]
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-1-5-21-1923240461-1905901954-2556564120-1001[profileimagepath]
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:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[name]

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[parsiname]
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: HKU\default\software\microsoft\windows\currentversion\explorer\user
shell folders[cache]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[default]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbscapiforcrack]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[3mu581d.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[*]
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: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[3mu581d.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[*]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[3mu581d.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[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[idnenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[preconnectlimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[preresolveimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[sqmhttpstreamrandomuploadpoolsize]
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\windows\currentversion\internet
settings[clientauthbuiltinui]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautopxyresultcache]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[displayscriptdownloadfailureui]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbscservername]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[utf8servernameres]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
Queries value: 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[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: HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttptnocachecheck]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasshttptnocachecheck]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[enablehttptrace]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrevving]
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[winsock_registry_version]
Queries value:

[illegible]

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[storserviceclassinfo]
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[storserviceclassinfo]
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\software\policies\microsoft\windows\currentversion\internet
settings[proxysettingsperuser]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[badproxyexpiretime]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[nonetautodial]
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\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: HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disablebranchcache]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[usefirstavailable]
Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[combinefalsestartdata]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablefalsestartblacklist]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enforce3pvalidity]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\service[enable]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6[winsock 2.0 provider id]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
Queries value: 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[autodetect]
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\{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}[parsiname]
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}[streamresource type]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-

6fba-4fcf-9d55-7b8e7f157091}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local appdata]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[cachelimit]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[parentfolder]

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

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

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cache\limit]
Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll]
Queries value: HKLM\software\microsoft\com3[com+enabled]
Queries value: HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
Queries value: HKLM\software\microsoft\ole[defaultaccesspermission]
Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[type]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[image path]
Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
Queries value: HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
Queries value: HKLM\software\microsoft\cryptography[machineguid]
Queries value: HKCR\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32[]
Queries value: HKCR\wow6432node\interface\{a168aad0-1674-49da-ad4f-
4f27df8760d0}\proxystubclsid32[]
Queries value: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}[]
Queries value: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\ole[maxsxshashcount]
Queries value: HKU\default\software\microsoft\windows\currentversion\explorer\user
shell folders[local appdata]
Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters[usedomainnamedevolution]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters[domainnamedevolutionlevel]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters[prioritize record data]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritize record data]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters[allowunqualifiedquery]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters[appendtomultilabelname]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters[screenbadtlds]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters[screenunreachableservers]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters[screendefaultservers]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters[dynamicserverqueryorder]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters[filterclusterip]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters[waitfornameerroronall]
Queries value: HKLM\system\currentcontrolset\services\dns\cache\parameters[usedns]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters[dnssecurenamequeryfallback]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters[enableadaforallnetworks]

Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[directaccessqueryorder]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[queryipmatching]
Queries value: HKLM\system\currentcontrolset\services\dns\parameters[usehostsfile]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[addrconfigcontrol]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[disablesmartnameresolution]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[preferlocaloverlowerbindingdns]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[querynetbtqdn]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[disablesmartprotocolreordering]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[udprecvbuffersize]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[registerprimaryname]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[registerreverselookup]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[registerwanadapters]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[registrationttl]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[registrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressesstoregister]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[updatesecuritylevel]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[updatetopleveldomainzones]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[downcasespncauseapiowneristoolazy]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[registrationoverwrite]
Queries value: HKLM\system\currentcontrolset\services\dns\parameters[maxcachesize]
Queries value: HKLM\system\currentcontrolset\services\dns\parameters[maxcachettl]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[maxnegativecachettl]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[adaptertimeoutlimit]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[serverprioritytimelimit]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[maxcachedsockets]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[enablemulticast]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[multicastresponderflags]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[multicastsenderflags]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[multicastsendermaxtimeout]
Queries value: HKLM\system\currentcontrolset\services\dns\parameters[dnstest]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[usecompartments]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters[cacheallcompartments]
Queries value:
HKLM\system\currentcontrolset\services\dns\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[newdhcprsvregistration]
 Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[directaccesspreferlocal]
 Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[disableidnencoding]
 Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[enableidnmapping]
 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:

HKCU\software\microsoft\windows\currentversion\internet
 settings[autoproxydetecttype]
 Queries value:

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

HKLM\system\currentcontrolset\services\winhttpautoproxysvc\parameters[proxydllfile]
 Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 settings[winhttplowercasehost]
 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[3mu581d.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[3mu581d.exe]
 Queries value:

HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_localmachine_lockdown[*]
 Queries value:

HKLM\software\policies\microsoft\windows\currentversion\internet
 settings[createuricachesize]
 Queries value:

HKCU\software\policies\microsoft\windows\currentversion\internet
 settings[createuricachesize]
 Queries value:

HKCU\software\microsoft\windows\currentversion\internet
 settings[createuricachesize]
 Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 settings[createuricachesize]
 Queries value:

HKLM\software\policies\microsoft\windows\currentversion\internet
 settings[enablepunycode]
 Queries value:

HKCU\software\policies\microsoft\windows\currentversion\internet
 settings[enablepunycode]
 Queries value:

HKCU\software\microsoft\windows\currentversion\internet
 settings[enablepunycode]
 Queries value:

HKCU\software\microsoft\windows\currentversion\internet
 settings\zonemap[autodetect]
 Queries value:

HKCU\software\microsoft\windows\currentversion\internet
 settings\zones\3[1a10]
 Queries value:

HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]
 Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[autodiald11]
 Queries value:

HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_zone_elevation[3mu581d.exe]
 Queries value:

HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_zone_elevation[*]
 Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
 Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
 Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[searchlist]
 Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[enabledhcp]
 Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[registrationenabled]

Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpv6domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpnameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[dhcpnameserver]
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[maxnumberofaddresstoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[enablemulticast]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[enableadapterdomainnameregistration]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[maxnumberofaddresstoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[enablemulticast]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
Sets/Creates value: HKLM\system\currentcontrolset\control\session
manager[pendingfilerenameoperations]
Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\run[1h6wzb8fuvux1d7fenotdr]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonintranet]

Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1409]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1609]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1406]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\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[enabledv8]
Sets/Creates value: HKCU\software\microsoft\internet
explorer\phishingfilter[shownservicedownballoon]
Sets/Creates value: HKCU\software\microsoft\internet
explorer\recovery[clearbrowsinghistoryonexit]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1409]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1609]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1406]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\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\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\5.0\cache\content[cacheprefix]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
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]