Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	43
Risk Level:	4
Date Processed:	2016-04-28 12:47:01 (UTC)
Processing Time:	61.93 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe"
Sample ID:	11
Type:	basic
Owner:	admin
Label:	83497c45d30bcb551f5f55f3f63b6fa1
Date Added:	2016-04-28 12:44:50 (UTC)
File Type:	PE32:win32:gui
File Size:	892928 bytes
MD5:	83497c45d30bcb551f5f55f3f63b6fa1
SHA256:	40932ac88b750f1f3077f2e50d9184de1c3b4914e92ceb64cfc4638c3d91ee14
Description:	None

Pattern Matching Results

3 Long sleep detected
3 Connects to local host
3 HTTP connection - response code 200 (success) [HTTP, POST, GET, web, network, response code]
4 Checks whether debugger is present

Process/Thread Events

```
  Creates process:          C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe
["C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe" ]
```

Named Object Events

```
  Creates mutex:            \Sessions\1\BaseNamedObjects\DBWinMutex
  Creates mutex:            \Sessions\1\BaseNamedObjects\!PrivacIE!SharedMemory!Mutex
  Creates mutex:            \Sessions\1\BaseNamedObjects\ZonesCounterMutex
  Creates mutex:            \Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex
  Creates mutex:            \Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex
  Creates mutex:            \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex
  Creates mutex:            \Sessions\1\BaseNamedObjects\_!MSFTHISTORY!_
  Creates mutex:
\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!temporary internet
files!content.ie5!
  Creates mutex:
\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!roaming!microsoft!windows!cookies!
  Creates mutex:
\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!history!history.ie5!
  Creates mutex:            \Sessions\1\BaseNamedObjects\WininetStartupMutex
  Creates mutex:            \Sessions\1\BaseNamedObjects\WininetConnectionMutex
  Creates mutex:            \Sessions\1\BaseNamedObjects\WininetProxyRegistryMutex
  Creates mutex:            \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
  Creates mutex:            \Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1
  Creates mutex:            \Sessions\1\BaseNamedObjects\!IETld!Mutex
  Creates mutex:            \Sessions\1\BaseNamedObjects\RasPbFile
  Creates mutex:            \Sessions\1\BaseNamedObjects\IESQMMUTEX_0_208
  Creates mutex:            \Sessions\1\BaseNamedObjects\MSIMGSIZECacheMutex
  Creates mutex:
\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!roaming!microsoft!windows!ietldcache!
  Creates event:            \KernelObjects\MaximumCommitCondition
  Creates event:            \Security\LSA_AUTHENTICATION_INITIALIZED
  Creates event:            \Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1
  Creates event:            \BaseNamedObjects\SvcctrlStartEvent_A3752DX
  Creates event:            \BaseNamedObjects\BFE_Notify_Event_{799dc87b-572e-4c35-9389-
76268ebfd260}
```

File System Events

```
  Creates:                  C:\Users\Admin
  Creates:                  C:\Users\Admin\AppData\Local
  Creates:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
  Creates:                  C:\Users\Admin\AppData\Roaming
  Creates:                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
  Creates:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\History
  Creates:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\104[1]
  Creates:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\property_front[1].aspx
  Creates:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\JMX.Frame.Common[1].js
  Creates:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
```

```
Files\Content.IE5\KQ5TVCON\JMX_AjaxControl[1].js
  Creates:               C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\JMX_FormValidator[1].js
  Creates:               C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\jquery-1.4.2.min[1].js
  Creates:               C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\client_ending[1].htm
  Creates:               C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\SRO-ending[1].jpg
  Creates:               C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\btn_facebook[1].jpg
  Opens:                 C:\Windows\Prefetch\83497C45D30BCB551F5F55F3F63B6-CCFC2B0F.pf
  Opens:                 C:\Windows\System32
  Opens:                 C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe.Local\
  Opens:                 C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af
  Opens:                 C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll
  Opens:                 C:\Windows\System32\sechost.dll
  Opens:                 C:\windows\temp\WINSPOOL.DRV
  Opens:                 C:\Windows\System32\winspool.drv
  Opens:                 C:\windows\temp\oledlg.dll
  Opens:                 C:\Windows\System32\oledlg.dll
  Opens:                 C:\Windows\System32\imm32.dll
  Opens:                 C:\Windows\System32\uxtheme.dll
  Opens:                 C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe.2.Manifest
  Opens:                 C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe.3.Manifest
  Opens:                 C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe.Config
  Opens:                 C:\Windows\Temp\83497c45d30bcb551f5f55f3f63b6fa1.exe
  Opens:                 C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe.1000.Manifest
  Opens:                 C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1ENU.dll
  Opens:                 C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1LOC.dll
  Opens:                 C:\Windows\Fonts\tahoma.ttf
  Opens:                 C:\windows\temp\dwmapi.dll
  Opens:                 C:\Windows\System32\dwmapi.dll
  Opens:                 C:\Windows\winhlp32.exe
  Opens:                 C:\Windows\System32\rpcss.dll
  Opens:                 C:\windows\temp\CRYPTBASE.dll
  Opens:                 C:\Windows\System32\cryptbase.dll
  Opens:                 C:\Windows\System32\ieframe.dll
  Opens:                 C:\Windows\System32\oleacc.dll
  Opens:                 C:\windows\temp\OLEACCRC.DLL
  Opens:                 C:\Windows\System32\oleaccrc.dll
  Opens:                 C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
  Opens:                 C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
  Opens:                 C:\Windows\WindowsShell.Manifest
  Opens:                 C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                 C:\Windows\System32\shell32.dll
  Opens:                 C:\windows\temp\apphelp.dll
  Opens:                 C:\Windows\System32\apphelp.dll
  Opens:                 C:\Windows\System32\en-US\ieframe.dll.mui
  Opens:                 C:\Windows\System32\mshtml.dll
  Opens:                 C:\Windows\System32\msls31.dll
  Opens:                 C:\Windows\System32\version.dll
  Opens:                 C:\windows\temp\ntmarta.dll
  Opens:                 C:\Windows\System32\ntmarta.dll
  Opens:                 C:\windows\temp\SspiCli.dll
  Opens:                 C:\Windows\System32\sspicli.dll
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
  Opens:                 C:\
  Opens:                 C:\Windows
  Opens:                 C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe:Zone.Identifier
  Opens:                 C:\windows\temp\profapi.dll
  Opens:                 C:\Windows\System32\profapi.dll
  Opens:                 C:\Users\Admin
  Opens:                 C:\Users\Admin\AppData\Local
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\desktop.ini
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\desktop.ini
  Opens:                 C:\Users\Admin\AppData\Roaming
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\History
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\index.dat
```

```
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
  Opens:                 C:\Windows\System32\wininet.dll
  Opens:                 C:\windows\temp\dnsapi.DLL
  Opens:                 C:\Windows\System32\dnsapi.dll
  Opens:                 C:\windows\temp\iphlpapi.DLL
  Opens:                 C:\Windows\System32\IPHLPAPI.DLL
  Opens:                 C:\windows\temp\WINNSI.DLL
  Opens:                 C:\Windows\System32\winnsi.dll
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\104[1]
  Opens:                 C:\Windows\System32\en-US\urlmon.dll.mui
  Opens:                 C:\windows\temp\RASAPI32.dll
  Opens:                 C:\Windows\System32\rasapi32.dll
  Opens:                 C:\windows\temp\rasman.dll
  Opens:                 C:\Windows\System32\rasman.dll
  Opens:                 C:\windows\temp\rtutils.dll
  Opens:                 C:\Windows\System32\rtutils.dll
  Opens:                 C:\ProgramData\Microsoft\Network\Connections\Pbk\
  Opens:                 C:\Windows\System32\ras
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk
  Opens:                 C:\windows\temp\sensapi.dll
  Opens:                 C:\Windows\System32\SensApi.dll
  Opens:                 C:\Windows\System32\nlaapi.dll
  Opens:                 C:\windows\temp\rasadhlp.dll
  Opens:                 C:\Windows\System32\rasadhlp.dll
  Opens:                 C:\Windows\System32\NapiNSP.dll
  Opens:                 C:\Windows\System32\pnrpnsp.dll
  Opens:                 C:\Windows\System32\mswsock.dll
  Opens:                 C:\Windows\System32\winrnr.dll
  Opens:                 C:\Windows\System32\WSHTCPIP.DLL
  Opens:                 C:\Windows\System32\wship6.dll
  Opens:                 C:\windows\temp\dhcpcsvc6.DLL
  Opens:                 C:\Windows\System32\dhcpcsvc6.dll
  Opens:                 C:\windows\temp\dhcpcsvc.DLL
  Opens:                 C:\Windows\System32\dhcpcsvc.dll
  Opens:                 C:\Windows\System32\drivers\etc\hosts
  Opens:                 C:\Windows\System32\FWPUCLNT.DLL
  Opens:                 C:\Windows\System32\netprofm.dll
  Opens:                 C:\windows\temp\CRYPTSP.dll
  Opens:                 C:\Windows\System32\cryptsp.dll
  Opens:                 C:\Windows\System32\rsaenh.dll
  Opens:                 C:\windows\temp\RpcRtRemote.dll
  Opens:                 C:\Windows\System32\RpcRtRemote.dll
  Opens:                 C:\Windows\System32\npmproxy.dll
  Opens:                 C:\Windows\System32\msimtf.dll
  Opens:                 C:\windows\temp\MLANG.dll
  Opens:                 C:\Windows\System32\mlang.dll
  Opens:                 C:\Windows\Fonts\times.ttf
  Opens:                 C:\Windows\System32\C_20127.NLS
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\property_front[1].aspx
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\JMX_AjaxControl[1].js
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\JMX.Frame.Common[1].js
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\jquery-1.4.2.min[1].js
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\JMX_FormValidator[1].js
  Opens:                 C:\Windows\System32\jscript.dll
  Opens:                 C:\Windows\System32\en-US\jscript.dll.mui
  Opens:                 C:\Windows\System32\en-US\KernelBase.dll.mui
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\client_ending[1].htm
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT
  Opens:                 C:\Windows\System32\en-US\mshtml.dll.mui
  Opens:                 C:\Windows\Fonts\StaticCache.dat
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache\index.dat
  Writes to:             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\104[1]
  Writes to:             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\property_front[1].aspx
  Writes to:             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\JMX_AjaxControl[1].js
  Writes to:             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\JMX.Frame.Common[1].js
  Writes to:             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\jquery-1.4.2.min[1].js
```

```
  Writes to:             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\JMX_FormValidator[1].js
  Writes to:             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\client_ending[1].htm
  Writes to:             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\SRO-ending[1].jpg
  Writes to:             C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\btn_facebook[1].jpg
  Reads from:            C:\Windows\System32\drivers\etc\hosts
  Reads from:            C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\jquery-1.4.2.min[1].js
  Reads from:            C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\JMX_FormValidator[1].js
  Reads from:            C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\JMX_AjaxControl[1].js
  Reads from:            C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\JMX.Frame.Common[1].js
  Reads from:            C:\Windows\Fonts\StaticCache.dat
```

Network Events

```
  DNS query:             wpad
  DNS query:             www.joymax.com
  DNS query:             file.joymax.com
  DNS query:             silkroadcp.joymax.com
  DNS query:             img.joymax.com
  DNS response:          www.joymax.com ⇒ 222.111.176.232
  DNS response:          file.joymax.com ⇒ 222.111.176.232
  DNS response:          silkroadcp.joymax.com ⇒ 121.128.133.11
  DNS response:          silkroadcp.joymax.com ⇒ 121.128.133.12
  DNS response:          img.joymax.com.gccdn.net ⇒ 14.0.55.3
  DNS response:          img.joymax.com.gccdn.net ⇒ 14.0.55.10
  Connects to:           127.0.0.1:56646
  Connects to:           222.111.176.232:80
  Connects to:           121.128.133.11:80
  Connects to:           14.0.55.3:80
  Sends data to:         0.0.0.0:5355
  Sends data to:         224.0.0.252:5355
  Sends data to:         8.8.8.8:53
  Sends data to:         127.0.0.1:56646
  Sends data to:         file.joymax.com:80 (222.111.176.232)
  Sends data to:         silkroadcp.joymax.com:80 (121.128.133.11)
  Sends data to:         img.joymax.com.gccdn.net:80 (14.0.55.3)
  Receives data from:    8.8.8.8:53
  Receives data from:    127.0.0.1:56646
  Receives data from:    file.joymax.com:80 (222.111.176.232)
  Receives data from:    silkroadcp.joymax.com:80 (121.128.133.11)
  Receives data from:    img.joymax.com.gccdn.net:80 (14.0.55.3)
```

Windows Registry Events

```
  Creates key:           HKCU\software\microsoft\windows\currentversion\internet settings
  Creates key:           HKLM\software\microsoft\tracing
  Creates key:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasapi32
  Creates key:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasmancs
  Creates key:           HKCU\software\microsoft\windows\currentversion\internet
settings\connections
  Creates key:           HKCU\software\microsoft\windows nt\currentversion\network\location
awareness
  Creates key:           HKLM\system\currentcontrolset\services\tcpip\parameters
  Creates key:           HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{228d30c5-2af6-45b6-bf55-65a88ac6a29a}
  Creates key:           HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{228d30c5-2af6-45b6-bf55-65a88ac6a29a}\a2-98-d5-56-33-71
  Creates key:           HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\a2-98-d5-56-33-71
  Creates key:           HKCU\software\microsoft\windows\currentversion\internet
settings\p3p\history
  Creates key:           HKCU\software\microsoft\windows script\settings
  Deletes value:         HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[proxybypass]
  Deletes value:         HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap[proxybypass]
  Deletes value:         HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[intranetname]
  Deletes value:         HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap[intranetname]
  Deletes value:         HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
  Deletes value:         HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
  Deletes value:         HKCU\software\microsoft\windows\currentversion\internet
```

```
settings[autoconfigurl]
  Opens key:              HKLM\system\currentcontrolset\control\session manager
  Opens key:              HKLM\system\currentcontrolset\control\terminal server
  Opens key:              HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:              HKLM\system\currentcontrolset\control\srp\gp\dll
  Opens key:              HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:              HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:              HKCU\
  Opens key:              HKCU\control panel\desktop\muicached\machinelanguageconfiguration
  Opens key:              HKLM\software\policies\microsoft\mui\settings
  Opens key:              HKCU\software\policies\microsoft\control panel\desktop
  Opens key:              HKCU\control panel\desktop\languageconfiguration
  Opens key:              HKCU\control panel\desktop
  Opens key:              HKCU\control panel\desktop\muicached
  Opens key:              HKLM\software\microsoft\windows\currentversion\sidebyside
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:              HKLM\system\currentcontrolset\control\nls\sorting\versions
  Opens key:              HKLM\system\currentcontrolset\control\error message instrument\
  Opens key:              HKLM\system\currentcontrolset\control\error message instrument
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\gre_initialize
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\compatibility32
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\ime compatibility
  Opens key:              HKLM\
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\windows
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\diagnostics
  Opens key:              HKLM\software\microsoft\ole
  Opens key:              HKLM\software\microsoft\ole\tracing
  Opens key:              HKCU\software\classes\
  Opens key:              HKCU\software\classes\clsid
  Opens key:              HKCR\clsid
  Opens key:              HKLM\software\microsoft\oleaut
  Opens key:              HKCU\software\microsoft\windows\currentversion\policies\explorer
  Opens key:              HKCU\software\microsoft\windows\currentversion\policies\network
  Opens key:              HKCU\software\microsoft\windows\currentversion\policies\comdlg32
  Opens key:              HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:              HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:              HKLM\system\currentcontrolset\control\nls\locale
  Opens key:              HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
  Opens key:              HKLM\system\currentcontrolset\control\nls\language groups
  Opens key:              HKLM\software\microsoft\com3
  Opens key:              HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
  Opens key:              HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
  Opens key:              HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\treatas
  Opens key:              HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas
  Opens key:              HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\progid
  Opens key:              HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid
  Opens key:              HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32
  Opens key:              HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32
  Opens key:              HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandler32
  Opens key:              HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler32
  Opens key:              HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandler
  Opens key:              HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler
  Opens key:              HKLM\software\microsoft\rpc
  Opens key:              HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:              HKLM\system\setup
  Opens key:              HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:              HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:              HKLM\software\microsoft\sqmclient\windows
  Opens key:              HKLM\system\currentcontrolset\services\crypt32
  Opens key:              HKLM\software\microsoft\windows\currentversion\internet settings
  Opens key:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:              HKCU\software\microsoft\windows\currentversion\internet settings
  Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
  Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
  Opens key:              HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:              HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:              HKLM\software\microsoft\internet explorer\main\featurecontrol
  Opens key:              HKCU\software\microsoft\internet explorer\main\featurecontrol
  Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
  Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
```

```
  Opens key:              HKCU\software\microsoft\internet explorer\main
  Opens key:              HKLM\software\microsoft\internet explorer\main
  Opens key:              HKLM\software\policies\microsoft\internet explorer\main
  Opens key:              HKCU\software\policies\microsoft\internet explorer\main
  Opens key:              HKLM\software\microsoft\windows\currentversion\policies\explorer
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\83497c45d30bcb551f5f55f3f63b6fa1.exe
  Opens key:              HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder
  Opens key:              HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder
  Opens key:              HKCU\software\microsoft\windows\currentversion\explorer\clsid\{871c5380-
42a0-1069-a2ea-08002b30309d}\shellfolder
  Opens key:              HKCU\software\microsoft\windows\currentversion\policies\nonenum
  Opens key:              HKLM\software\microsoft\windows\currentversion\policies\nonenum
  Opens key:              HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32
  Opens key:              HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32
  Opens key:              HKLM\software\microsoft\windows\currentversion\shell extensions\blocked
  Opens key:              HKCU\software\microsoft\windows\currentversion\shell extensions\blocked
  Opens key:              HKLM\system\currentcontrolset\control\session manager\appcompatibility
  Opens key:              HKLM\software\policies\microsoft\windows\appcompat
  Opens key:              HKCU\software\microsoft\windows\currentversion\shell extensions\cached
  Opens key:              HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
  Opens key:              HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
  Opens key:              HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\treatas
  Opens key:              HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas
  Opens key:              HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\progid
  Opens key:              HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\progid
  Opens key:              HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprochandler32
  Opens key:              HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler32
  Opens key:              HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprochandler
  Opens key:              HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{871c5380-42a0-1069-
a2ea-08002b30309d}
  Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_protocol
  Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_protocol
  Opens key:              HKLM\software\policies\microsoft\internet explorer\browseremulation
  Opens key:              HKCU\software\policies\microsoft\internet explorer\browseremulation
  Opens key:              HKLM\system\currentcontrolset\control\cmf\config
  Opens key:              HKCU\software\classes\protocols\name-space handler\
  Opens key:              HKCR\protocols\name-space handler
  Opens key:              HKCU\software\classes\protocols\name-space handler\res\
  Opens key:              HKCR\protocols\name-space handler\res
  Opens key:              HKCU\software\classes\protocols\name-space handler\*\
  Opens key:              HKCR\protocols\name-space handler\*
  Opens key:              HKCU\software\classes\protocols\handler\res
  Opens key:              HKCR\protocols\handler\res
  Opens key:              HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:              HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:              HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-
00aa00bdce0b}\treatas
  Opens key:              HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\treatas
  Opens key:              HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-
00aa00bdce0b}\progid
  Opens key:              HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\progid
  Opens key:              HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
  Opens key:              HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
  Opens key:              HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
  Opens key:              HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32
  Opens key:              HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler
  Opens key:              HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprochandler
  Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
  Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
  Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
  Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
  Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_aria_support
  Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_aria_support
```

```
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_private_font_setting
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_private_font_setting
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_css_show_hide_events
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_css_show_hide_events
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_expanduri_bypass
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_expanduri_bypass
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_crash_recovery_save_kb978454
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_crash_recovery_save_kb978454
  Opens key:                 HKCU\software\microsoft\windows nt\currentversion\windows
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fls
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fls
  Opens key:                 HKLM\software\microsoft\windows\currentversion\app paths\outlook.exe
  Opens key:                 HKLM\software\microsoft\internet explorer\application compatibility
  Opens key:                 HKLM\software\policies\microsoft\internet explorer\domstorage
  Opens key:                 HKCU\software\policies\microsoft\internet explorer\domstorage
  Opens key:                 HKCU\software\microsoft\internet explorer\domstorage
  Opens key:                 HKLM\software\microsoft\internet explorer\domstorage
  Opens key:                 HKLM\software\policies\microsoft\internet explorer\safety\privacie
  Opens key:                 HKCU\software\policies\microsoft\internet explorer\safety\privacie
  Opens key:                 HKCU\software\microsoft\internet explorer\safety\privacie
  Opens key:                 HKLM\software\microsoft\internet explorer\safety\privacie
  Opens key:                 HKLM\system\currentcontrolset\control\lsa\accessproviders
  Opens key:                 HKLM\system\currentcontrolset\services\ldap
  Opens key:                 HKLM\software\microsoft\internet explorer\mediatypeclass
  Opens key:                 HKLM\software\microsoft\windows\currentversion\internet
settings\accepted documents
  Opens key:                 HKLM\software\microsoft\windows\currentversion\policies\ratings
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
  Opens key:                 HKLM\software\policies
  Opens key:                 HKCU\software\policies
  Opens key:                 HKCU\software
  Opens key:                 HKLM\software
  Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\protocoldefaults\
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                HKLM\software\policies\microsoft\internet explorer
  Opens key:                HKLM\software\policies\microsoft\internet explorer\security
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\zones\
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
```

```
settings\lockdown_zones\0
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
  Opens key:                 HKLM\software\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\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\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\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\classes\protocols\name-space handler\c\
  Opens key:                 HKCR\protocols\name-space handler\c
  Opens key:                 HKCU\software\classes\protocols\handler\c
  Opens key:                 HKCR\protocols\handler\c
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}\propertybag
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}\propertybag
  Opens key:                 HKCU\software\microsoft\internet explorer
  Opens key:                 HKLM\software\microsoft\internet explorer
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_res_to_lmz
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_res_to_lmz
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_load_shdoclc_resources
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_load_shdoclc_resources
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_feeds
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_feeds
  Opens key:                 HKCU\software\classes\protocols\filter\text/html
  Opens key:                 HKCR\protocols\filter\text/html
  Opens key:                 HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
```

```
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
  Opens key:                 HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
  Opens key:                 HKLM\software\policies\microsoft\windows\explorer
  Opens key:                 HKCU\software\policies\microsoft\windows\explorer
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}\propertybag
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}\propertybag
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
2160590473-689474908-1361669368-1002
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
  Opens key:                 HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}\propertybag
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
  Opens key:                 HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}\propertybag
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
  Opens key:                 HKLM\software\microsoft\internet
```

```
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
   Opens key:                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
   Opens key:                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
   Opens key:                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
   Opens key:                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
   Opens key:                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
   Opens key:                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
   Opens key:                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
   Opens key:                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
   Opens key:                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
   Opens key:                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
   Opens key:                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
   Opens key:                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
   Opens key:                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
   Opens key:                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
   Opens key:                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
   Opens key:                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
   Opens key:                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
   Opens key:                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
   Opens key:                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
   Opens key:                    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\14993e33
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017
```

```
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
  Opens key:
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:                HKCU\software\microsoft\windows\currentversion\internet settings\wpad
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:                HKLM\software\microsoft\windows\windows error reporting\wmr
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject
  Opens key:                HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
  Opens key:                HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
  Opens key:                HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\treatas
  Opens key:                HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas
  Opens key:                HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\progid
  Opens key:                HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid
  Opens key:                HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32
  Opens key:                HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprochandler32
  Opens key:                HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprochandler
  Opens key:                HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_manage_script_circular_refs
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_manage_script_circular_refs
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload
  Opens key:                HKLM\software\microsoft\internet explorer\security\floppy access
  Opens key:                HKCU\software\microsoft\internet explorer\security\adv addrbar spoof
detection
  Opens key:                HKLM\software\microsoft\internet explorer\security\adv addrbar spoof
detection
  Opens key:                HKCU\software\classes\protocols\name-space handler\about\
  Opens key:                HKCR\protocols\name-space handler\about
  Opens key:                HKCU\software\classes\protocols\handler\about
  Opens key:                HKCR\protocols\handler\about
  Opens key:                HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:                HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:                HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\treatas
  Opens key:                HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas
  Opens key:                HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\progid
  Opens key:                HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\progid
  Opens key:                HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
  Opens key:                HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
  Opens key:                HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler
  Opens key:                HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandler
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_document_compatible_mode
```

```
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_document_compatible_mode
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
  Opens key:                 HKLM\software\policies\microsoft\internet explorer\zoom
  Opens key:                 HKCU\software\policies\microsoft\internet explorer\zoom
  Opens key:                 HKCU\software\microsoft\internet explorer\zoom
  Opens key:                 HKLM\software\microsoft\internet explorer\zoom
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_weboc_document_zoom
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_weboc_document_zoom
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ipersistmoniker_load_redirected_url_kb976425
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_ipersistmoniker_load_redirected_url_kb976425
  Opens key:                 HKCU\software\policies\microsoft\internet explorer
  Opens key:                 HKCU\software\microsoft\internet explorer\international
  Opens key:                 HKLM\software\policies\microsoft\internet explorer\international\scripts
  Opens key:                 HKCU\software\microsoft\internet explorer\international\scripts
  Opens key:                 HKLM\software\microsoft\internet explorer\international\scripts
  Opens key:                 HKLM\software\policies\microsoft\internet explorer\settings
  Opens key:                 HKCU\software\microsoft\internet explorer\settings
  Opens key:                 HKLM\software\microsoft\internet explorer\settings
  Opens key:                 HKCU\software\microsoft\internet explorer\styles
  Opens key:                 HKCU\software\microsoft\windows\currentversion\policies\activedesktop
  Opens key:                 HKCU\software\microsoft\windows\currentversion\policies
  Opens key:                 HKCU\software\microsoft\internet explorer\pagesetup
  Opens key:                 HKCU\software\microsoft\internet explorer\menuext
  Opens key:                 HKCU\software\microsoft\internet explorer\menuext\%s
  Opens key:                 HKLM\system\currentcontrolset\control\nls\codepage
  Opens key:                 HKCU\software\microsoft\internet explorer\international\scripts\3
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\travellog
  Opens key:                 HKLM\software\microsoft\windows\currentversion\explorer\travellog
  Opens key:                 HKLM\software\microsoft\internet explorer\version vector
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_sslux
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_sslux
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
  Opens key:                 HKLM\software\microsoft\windows\currentversion\internet settings\zones\0
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\zones
  Opens key:
HKLM\software\microsoft\ctf\compatibility\83497c45d30bcb551f5f55f3f63b6fa1.exe
  Opens key:                 HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
  Opens key:                 HKLM\software\microsoft\ctf\
  Opens key:                 HKLM\software\microsoft\ctf\knownclasses
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_compat_logging
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_compat_logging
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
  Opens key:                 HKCU\software\microsoft\internet explorer\ietld
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_shim_mshelp_combine
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_shim_mshelp_combine
  Opens key:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasapi32
  Opens key:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasmancs
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\profilelist
  Opens key:              HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
  Opens key:              HKLM\system\currentcontrolset\control\sqmservicelist
  Opens key:              HKLM\software\microsoft\sqmclient\windows\disabledsessions\
  Opens key:              HKU\
  Opens key:              HKCU\software\classes\autoproxytypes
  Opens key:              HKCR\autoproxytypes
  Opens key:              HKCU\software\classes\autoproxytypes\application/x-internet-signup
  Opens key:              HKCR\autoproxytypes\application/x-internet-signup
  Opens key:              HKCU\software\classes\autoproxytypes\application/x-ns-proxy-autoconfig
  Opens key:              HKCR\autoproxytypes\application/x-ns-proxy-autoconfig
  Opens key:              HKLM\system\currentcontrolset\services\dnscache\parameters
  Opens key:              HKLM\software\policies\microsoft\windows nt\dnsclient
  Opens key:              HKLM\system\currentcontrolset\services\dns
  Opens key:              HKLM\software\policies\microsoft\system\dnsclient
  Opens key:              HKLM\system\currentcontrolset\services\winsock\parameters
  Opens key:              HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
  Opens key:              HKLM\system\currentcontrolset\services\psched\parameters\winsock
  Opens key:              HKLM\system\currentcontrolset\services\winsock\setup migration\providers
  Opens key:              HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched
  Opens key:              HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
  Opens key:              HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
  Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
  Opens key:              HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
  Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_isolate_named_windows
  Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_isolate_named_windows
  Opens key:              HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
  Opens key:              HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache
  Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}
  Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_binary_caller_service_provider
  Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_binary_caller_service_provider
  Opens key:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\url history
  Opens key:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\url history
  Opens key:              HKCU\software\microsoft\windows\currentversion\internet settings\url
history
  Opens key:              HKLM\software\microsoft\windows\currentversion\internet settings\url
history
  Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_codepage_inherit
  Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_codepage_inherit
  Opens key:              HKCU\software\classes\protocols\name-space handler\http\
  Opens key:              HKCR\protocols\name-space handler\http
  Opens key:              HKCU\software\microsoft\windows\currentversion\internet settings\user
agent
  Opens key:              HKLM\software\microsoft\windows\currentversion\internet settings\user
agent
  Opens key:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent
  Opens key:              HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent
  Opens key:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\user agent
  Opens key:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\user agent
  Opens key:              HKLM\software\microsoft\windows\currentversion\internet settings\user
agent\ua tokens
  Opens key:              HKLM\software\microsoft\windows\currentversion\internet settings\user
agent\pre platform
  Opens key:              HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\pre platform
  Opens key:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\pre platform
  Opens key:              HKLM\software\microsoft\windows\currentversion\internet settings\user
agent\post platform
  Opens key:              HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\post platform
  Opens key:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\post platform
  Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver
  Opens key:              HKLM\software\microsoft\internet
```

```
explorer\main\featurecontrol\feature_maxconnectionsperserver
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}
  Opens key:                HKCU\software\microsoft\windows\currentversion\urlmon settings
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
  Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{8ff7f47b-d658-4061-baea-
1709a0196aed}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{7b9cb019-1924-49a5-867c-
a68f334c8d34}
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\linkage
  Opens key:                HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}
  Opens key:                HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}
  Opens key:                HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\treatas
  Opens key:                HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\treatas
  Opens key:                HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\progid
  Opens key:                HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\progid
  Opens key:                HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprocserver32
  Opens key:                HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprochandler32
  Opens key:                HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprochandler
  Opens key:                HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\inprochandler
  Opens key:                HKLM\software\microsoft\rpc\extensions
  Opens key:                HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}
  Opens key:                HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}
  Opens key:                HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\treatas
  Opens key:                HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\treatas
  Opens key:                HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\progid
  Opens key:                HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\progid
  Opens key:                HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprocserver32
  Opens key:                HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprochandler32
  Opens key:                HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprochandler
  Opens key:                HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprochandler
  Opens key:                HKCU\software\classes\appid\83497c45d30bcb551f5f55f3f63b6fa1.exe
  Opens key:                HKCR\appid\83497c45d30bcb551f5f55f3f63b6fa1.exe
  Opens key:                HKLM\software\microsoft\ole\appcompat
  Opens key:                HKLM\system\currentcontrolset\control\lsa
  Opens key:                HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
  Opens key:                HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
  Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
  Opens key:                HKLM\software\policies\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography\offload
  Opens key:                HKCU\software\classes\interface\{00000134-0000-0000-c000-000000000046}
  Opens key:                HKCR\interface\{00000134-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                HKCR\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
  Opens key:                HKLM\system\currentcontrolset\services\bfe
  Opens key:                HKCU\software\classes\interface\{d0074ffd-570f-4a9b-8d69-199fdba5723b}
  Opens key:                HKCR\interface\{d0074ffd-570f-4a9b-8d69-199fdba5723b}
  Opens key:                HKCU\software\classes\interface\{d0074ffd-570f-4a9b-8d69-
199fdba5723b}\proxystubclsid32
  Opens key:                HKCR\interface\{d0074ffd-570f-4a9b-8d69-199fdba5723b}\proxystubclsid32
  Opens key:                HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}
  Opens key:                HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}
  Opens key:                HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\treatas
  Opens key:                HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\treatas
  Opens key:                HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\progid
  Opens key:                HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\progid
  Opens key:                HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32
  Opens key:                HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprochandler32
  Opens key:                HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprochandler
  Opens key:                HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprochandler
  Opens key:                HKCU\software\classes\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406}
  Opens key:                HKCR\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406}
  Opens key:                HKCU\software\classes\interface\{26656eaa-54eb-4e6f-8f85-
4f0ef901a406}\proxystubclsid32
  Opens key:                HKCR\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}
  Opens key:                HKCR\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}
  Opens key:                HKCU\software\classes\interface\{8a40a45d-055c-4b62-abd7-
6d613e2ceaec}\proxystubclsid32
  Opens key:                HKCR\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{55272a00-42cb-11ce-8135-00aa004bb851}
  Opens key:                HKCR\interface\{55272a00-42cb-11ce-8135-00aa004bb851}
  Opens key:                HKCU\software\classes\interface\{55272a00-42cb-11ce-8135-
00aa004bb851}\proxystubclsid32
  Opens key:                HKCR\interface\{55272a00-42cb-11ce-8135-00aa004bb851}\proxystubclsid32
  Opens key:                HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
  Opens key:                HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
  Opens key:                HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\treatas
  Opens key:                HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\treatas
  Opens key:                HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\progid
  Opens key:                HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\progid
  Opens key:                HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32
  Opens key:                HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprochandler32
  Opens key:                HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprochandler
  Opens key:                HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprochandler
  Opens key:                HKCU\software\classes\interface\{bcd1de7e-2db1-418b-b047-4a74e101f8c1}
  Opens key:                HKCR\interface\{bcd1de7e-2db1-418b-b047-4a74e101f8c1}
  Opens key:                HKCU\software\classes\interface\{bcd1de7e-2db1-418b-b047-
4a74e101f8c1}\proxystubclsid32
  Opens key:                HKCR\interface\{bcd1de7e-2db1-418b-b047-4a74e101f8c1}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}
  Opens key:                HKCR\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}
  Opens key:                HKCU\software\classes\interface\{2a1c9eb2-df62-4154-b800-
63278fcb8037}\proxystubclsid32
  Opens key:                HKCR\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}\proxystubclsid32
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{228d30c5-2af6-45b6-bf55-65a88ac6a29a}
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_legacy_compression
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_legacy_compression
  Opens key:                HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}
  Opens key:                HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}
  Opens key:                HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\treatas
  Opens key:                HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\treatas
  Opens key:                HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\progid
  Opens key:                HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\progid
  Opens key:                HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32
  Opens key:                HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprochandler32
  Opens key:                HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprochandler
```

```
  Opens key:                 HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprochandler
  Opens key:                 HKCU\software\classes\protocols\name-space handler
  Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\
  Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\
  Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\
  Opens key:                 HKLM\software\policies\microsoft\internet explorer\restrictions
  Opens key:                 HKCU\software\policies\microsoft\internet explorer\restrictions
  Opens key:                 HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}
  Opens key:                 HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}
  Opens key:                 HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\treatas
  Opens key:                 HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\treatas
  Opens key:                 HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\progid
  Opens key:                 HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\progid
  Opens key:                 HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32
  Opens key:                 HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32
  Opens key:                 HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprochandler32
  Opens key:                 HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandler32
  Opens key:                 HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprochandler
  Opens key:                 HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandler
  Opens key:                 HKCU\software\policies\microsoft\internet explorer\control panel
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
  Opens key:                 HKLM\software\policies\microsoft\internet explorer\recovery
  Opens key:                 HKCU\software\microsoft\internet explorer\recovery
  Opens key:                 HKCU\software\microsoft\internet explorer\feed discovery
  Opens key:                 HKLM\software\microsoft\internet explorer\feed discovery
  Opens key:                 HKCU\software\microsoft\ftp
  Opens key:                 HKLM\system\currentcontrolset\services\netbt\linkage
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\p3p\history\joymax.com
  Opens key:                 HKCU\software\classes\mime\database\content type\text/html; charset=utf-
8
  Opens key:                 HKCR\mime\database\content type\text/html; charset=utf-8
  Opens key:                 HKCU\software\classes\mime\database\content type\text/html
  Opens key:                 HKCR\mime\database\content type\text/html
  Opens key:                 HKCU\software\classes\protocols\filter\text/html; charset=utf-8
  Opens key:                 HKCR\protocols\filter\text/html; charset=utf-8
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown
  Opens key:                 HKCU\software\classes\mime\database\content type\application/x-
javascript
  Opens key:                 HKCR\mime\database\content type\application/x-javascript
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_script
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_script
  Opens key:                 HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
  Opens key:                 HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
  Opens key:                 HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\treatas
  Opens key:                 HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\treatas
  Opens key:                 HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\progid
  Opens key:                 HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\progid
  Opens key:                 HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32
  Opens key:                 HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32
  Opens key:                 HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprochandler32
  Opens key:                 HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprochandler32
  Opens key:                 HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprochandler
```

```
  Opens key:                HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprochandler
  Opens key:                HKLM\software\microsoft\windows script\features
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_windowedselectcontrol
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_windowedselectcontrol
  Opens key:                HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:                HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:                HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-
00aa00bdce0b}\treatas
  Opens key:                HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\treatas
  Opens key:                HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-
00aa00bdce0b}\progid
  Opens key:                HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\progid
  Opens key:                HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
  Opens key:                HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
  Opens key:                HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler
  Opens key:                HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\inprochandler
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_xmlhttp
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_xmlhttp
  Opens key:                HKLM\software\microsoft\internet explorer\abouturls
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_about_protocol_ie7
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_about_protocol_ie7
  Opens key:                HKLM\software\policies\microsoft\internet explorer\dxtrans
  Opens key:                HKCU\software\microsoft\internet explorer\dxtrans
  Opens key:                HKLM\software\microsoft\internet explorer\dxtrans
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_scripturl_mitigation
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_scripturl_mitigation
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\ms shell dlg
  Opens key:                HKCU\software\classes\mime\database\content type\image/jpeg
  Opens key:                HKCR\mime\database\content type\image/jpeg
  Opens key:                HKLM\software\policies\microsoft\internet explorer\services
  Opens key:                HKCU\software\microsoft\internet explorer\services
  Opens key:                HKLM\software\policies\microsoft\internet explorer\activities
  Opens key:                HKCU\software\microsoft\internet explorer\activities
  Opens key:                HKLM\software\microsoft\internet explorer\activities
  Opens key:                HKLM\software\policies\microsoft\internet
explorer\infodelivery\restrictions
  Opens key:                HKCU\software\policies\microsoft\internet
explorer\infodelivery\restrictions
  Opens key:                HKLM\software\policies\microsoft\internet explorer\suggested sites
  Opens key:                HKCU\software\microsoft\internet explorer\suggested sites
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:            HKCU\control panel\desktop[preferreduilanguages]
  Queries value:            HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\versions[]
  Queries value:            HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\compatibility32[83497c45d30bcb551f5f55f3f63b6fa1]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:              HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:              HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[en]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Queries value:              HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:              HKLM\software\microsoft\com3[com+enabled]
  Queries value:              HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid[]
  Queries value:              HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[]
  Queries value:              HKCR\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32[]
  Queries value:              HKCR\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[threadingmodel]
  Queries value:              HKLM\software\microsoft\ole[maxsxshashcount]
  Queries value:              HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:              HKLM\system\setup[oobeinprogress]
  Queries value:              HKLM\system\setup[systemsetupinprogress]
  Queries value:              HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:              HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
  Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
  Queries value:              HKLM\software\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\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:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[*]
  Queries value:              HKCU\software\microsoft\internet explorer\main[frametabwindow]
  Queries value:              HKLM\software\microsoft\internet explorer\main[frametabwindow]
  Queries value:              HKCU\software\microsoft\internet explorer\main[framemerging]
  Queries value:              HKLM\software\microsoft\internet explorer\main[framemerging]
  Queries value:              HKCU\software\microsoft\internet explorer\main[sessionmerging]
  Queries value:              HKLM\software\microsoft\internet explorer\main[sessionmerging]
  Queries value:              HKCU\software\microsoft\internet explorer\main[admintabprocs]
  Queries value:              HKLM\software\microsoft\internet explorer\main[admintabprocs]
  Queries value:              HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
  Queries value:              HKLM\software\microsoft\internet explorer\main[tabprocgrowth]
  Queries value:              HKLM\software\microsoft\internet explorer\main[navigationdelay]
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[attributes]
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[callforattributes]
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[restrictedattributes]
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsfordisplay]
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[hidefolderverbs]
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[usedrophandler]
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsforparsing]
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsparsedisplayname]
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[queryforoverlay]
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[mapnetdriveverbs]
```

```
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[queryforinfotip]
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[hideinwebview]
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[hideondesktopperuser]
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsaliasednotifications]
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsuniversaldelegate]
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[nofilefolderjunction]
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[pintonamespacetree]
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[hasnavigationenum]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\clsid\{871c5380-
42a0-1069-a2ea-08002b30309d}\shellfolder[attributes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{871c5380-42a0-1069-a2ea-
08002b30309d}]
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[]
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[loadwithoutcom]
  Queries value:              HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}
0xffff]
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[]
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[threadingmodel]
  Queries value:              HKLM\system\currentcontrolset\control\cmf\config[system]
  Queries value:              HKCR\protocols\handler\res[clsid]
  Queries value:              HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}[]
  Queries value:              HKCR\clsid\{3050f3bc-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
  Queries value:              HKCR\clsid\{3050f3bc-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[*]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching[*]
  Queries value:              HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
  Queries value:              HKLM\system\currentcontrolset\control\wmi\security[0cfe0455-93ba-440d-
a3fe-553973d0b723]
  Queries value:              HKLM\system\currentcontrolset\control\wmi\security[797fabac-7b58-4796-
b924-d51178a59ce4]
  Queries value:              HKLM\system\currentcontrolset\control\wmi\security[9e3b3947-ca5d-4614-
91a2-7b624e0e7244]
  Queries value:              HKLM\software\microsoft\internet explorer\application
compatibility[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:              HKCU\software\microsoft\internet explorer\domstorage[totallimit]
  Queries value:              HKCU\software\microsoft\internet explorer\domstorage[domainlimit]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
  Queries value:              HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
  Queries value:              HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
  Queries value:              HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
  Queries value:              HKLM\software\microsoft\windows\currentversion\policies\ratings[key]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[urlencoding]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[*]
  Queries value:              HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[flags]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[flags]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[flags]
```

```
  Queries value:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
  Queries value:              HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
  Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[category]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[name]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[parentfolder]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[description]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[relativepath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[parsingname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[infotip]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[localizedname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[icon]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[security]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[streamresource]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[streamresourcetype]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[localredirectonly]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[roamable]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[precreate]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[stream]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[publishexpandedpath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[attributes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[foldertypeid]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[initfolderhandler]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[category]
```

```
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[name]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[parentfolder]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[description]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[relativepath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[parsingname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[infotip]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[localizedname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[icon]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[security]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[streamresource]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[streamresourcetype]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[localredirectonly]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[roamable]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[precreate]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[stream]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[publishexpandedpath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[attributes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[foldertypeid]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[initfolderhandler]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
  Queries value:              HKCU\software\microsoft\internet explorer[no3dborder]
  Queries value:              HKLM\software\microsoft\internet explorer[no3dborder]
  Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[urlencoding]
  Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[urlencoding]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[*]
  Queries value:              HKLM\software\microsoft\ole[maximumallowedallocationsize]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_res_to_lmz[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_res_to_lmz[*]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing[*]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[istextplainhonored]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_feeds[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:              HKLM\software\microsoft\internet
```

```
explorer\main\featurecontrol\feature_feeds[*]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[signature]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[category]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[name]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[parentfolder]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[description]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[relativepath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[parsingname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[infotip]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[localizedname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[icon]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[security]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[streamresource]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[streamresourcetype]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[localredirectonly]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[roamable]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[precreate]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[stream]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[publishexpandedpath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[attributes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[foldertypeid]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[initfolderhandler]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local appdata]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[category]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[name]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[parentfolder]
  Queries value:
```

```
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[description]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[relativepath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[parsingname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[infotip]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[localizedname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[icon]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[security]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[streamresource]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[streamresourcetype]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[localredirectonly]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[roamable]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[precreate]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[stream]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[publishexpandedpath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[attributes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[foldertypeid]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[initfolderhandler]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
2160590473-689474908-1361669368-1002[profileimagepath]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cacheprefix]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cachelimit]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[category]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[name]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[parentfolder]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[description]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[relativepath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[parsingname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[infotip]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[localizedname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[icon]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[security]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[streamresource]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[streamresourcetype]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[localredirectonly]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[roamable]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[precreate]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[stream]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[publishexpandedpath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[attributes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[foldertypeid]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[initfolderhandler]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cachelimit]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[category]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[name]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[parentfolder]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[description]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[relativepath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[parsingname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[infotip]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[localizedname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[icon]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[security]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[streamresource]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[streamresourcetype]
```

```
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[localredirectonly]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[roamable]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[precreate]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[stream]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[publishexpandedpath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[attributes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[foldertypeid]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[initfolderhandler]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacherepair]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachepath]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheprefix]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheoptions]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacherepair]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachepath]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
  Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
```

```
settings[secureprotocols]
  Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
  Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
  Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
  Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
  Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disablebasicoverclearchannel]
  Queries value:              HKCU\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
  Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
  Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[displayscriptdownloadfailureui]
  Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsservername]
  Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsapiforcrack]
  Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[utf8servernameres]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[connectretries]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
```

```
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
  Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
```

```
settings[alwaysdrainonredirect]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[tcpautotuning]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
```

```
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\wpad[wpadoverride]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[nonetautodial]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[badproxyexpirestime]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[disablebranchcache]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
  Queries value:            HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[*]
  Queries value:            HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[]
  Queries value:            HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[]
  Queries value:            HKCR\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[]
  Queries value:            HKCR\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32[threadingmodel]
  Queries value:            HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinset]
  Queries value:            HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrolldelay]
  Queries value:            HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinterval]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[*]
  Queries value:            HKCR\protocols\handler\about[clsid]
  Queries value:            HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}[]
  Queries value:            HKCR\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
  Queries value:            HKCR\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2106]
  Queries value:            HKCU\software\microsoft\internet explorer\zoom[zoomdisabled]
  Queries value:            HKLM\software\policies\microsoft\internet explorer[smartdithering]
  Queries value:            HKCU\software\microsoft\internet explorer[smartdithering]
  Queries value:            HKCU\software\microsoft\internet explorer[rtfconverterflags]
  Queries value:            HKCU\software\microsoft\internet explorer\main[usecleartype]
  Queries value:            HKCU\software\microsoft\internet explorer\main[page_transitions]
  Queries value:            HKCU\software\microsoft\internet explorer\main[use_dlgbox_colors]
  Queries value:            HKCU\software\microsoft\internet explorer\main[anchor underline]
  Queries value:            HKCU\software\microsoft\internet explorer\main[css_compat]
  Queries value:            HKCU\software\microsoft\internet explorer\main[expand alt text]
  Queries value:            HKCU\software\microsoft\internet explorer\main[display inline images]
  Queries value:            HKCU\software\microsoft\internet explorer\main[display inline videos]
  Queries value:            HKLM\software\microsoft\internet explorer\main[display inline videos]
  Queries value:            HKCU\software\microsoft\internet explorer\main[play_background_sounds]
  Queries value:            HKCU\software\microsoft\internet explorer\main[play_animations]
  Queries value:            HKCU\software\microsoft\internet explorer\main[print_background]
  Queries value:            HKCU\software\microsoft\internet explorer\main[use stylesheets]
  Queries value:            HKCU\software\microsoft\internet explorer\main[smoothscroll]
  Queries value:            HKCU\software\microsoft\internet explorer\main[xmlhttp]
  Queries value:            HKCU\software\microsoft\internet explorer\main[show image placeholders]
  Queries value:            HKCU\software\microsoft\internet explorer\main[disable script debugger]
  Queries value:            HKCU\software\microsoft\internet explorer\main[disablescriptdebuggerie]
  Queries value:            HKCU\software\microsoft\internet explorer\main[move system caret]
  Queries value:            HKCU\software\microsoft\internet explorer\main[force offscreen
composition]
  Queries value:            HKCU\software\microsoft\internet explorer\main[enable autoimageresize]
  Queries value:            HKCU\software\microsoft\internet explorer\main[usethemes]
  Queries value:            HKCU\software\microsoft\internet explorer\main[usehr]
  Queries value:            HKCU\software\microsoft\internet explorer\main[q300829]
  Queries value:            HKCU\software\microsoft\internet explorer\main[cleanup htcs]
  Queries value:            HKCU\software\microsoft\internet explorer\main[xdomainrequest]
  Queries value:            HKLM\software\microsoft\internet explorer\main[xdomainrequest]
  Queries value:            HKCU\software\microsoft\internet explorer\main[domstorage]
  Queries value:            HKCU\software\microsoft\internet
explorer\international[default_codepage]
  Queries value:            HKCU\software\microsoft\internet explorer\international[autodetect]
  Queries value:            HKCU\software\microsoft\internet
explorer\international\scripts[default_iefontsizeprivate]
  Queries value:            HKCU\software\microsoft\internet explorer\settings[anchor color]
  Queries value:            HKCU\software\microsoft\internet explorer\settings[anchor color visited]
  Queries value:            HKCU\software\microsoft\internet explorer\settings[anchor color hover]
  Queries value:            HKCU\software\microsoft\internet explorer\settings[always use my colors]
  Queries value:            HKCU\software\microsoft\internet explorer\settings[always use my font
size]
  Queries value:            HKCU\software\microsoft\internet explorer\settings[always use my font
face]
  Queries value:            HKCU\software\microsoft\internet explorer\settings[disable visited
hyperlinks]
  Queries value:            HKCU\software\microsoft\internet explorer\settings[use anchor hover
color]
  Queries value:            HKCU\software\microsoft\internet explorer\settings[miscflags]
  Queries value:            HKCU\software\microsoft\windows\currentversion\policies[allow
programmatic cut_copy_paste]
  Queries value:            HKLM\software\policies\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
  Queries value:            HKCU\software\policies\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
  Queries value:            HKCU\software\microsoft\internet explorer\pagesetup[print_background]
  Queries value:            HKLM\system\currentcontrolset\control\nls\codepage[950]
  Queries value:            HKCU\software\microsoft\internet
explorer\international\scripts\3[iefontsize]
  Queries value:            HKCU\software\microsoft\internet
explorer\international\scripts\3[iefontsizeprivate]
  Queries value:            HKCU\software\microsoft\internet
explorer\international\scripts\3[iepropfontname]
  Queries value:            HKCU\software\microsoft\internet
explorer\international\scripts\3[iefixedfontname]
  Queries value:            HKCU\software\microsoft\internet explorer\international[acceptlanguage]
  Queries value:            HKLM\software\microsoft\internet explorer\version vector[ie]
  Queries value:            HKLM\software\microsoft\internet explorer\version vector[vml]
  Queries value:            HKLM\software\microsoft\internet explorer\version vector[windowsedition]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation[*]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_sslux[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_sslux[*]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation[*]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[2700]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings\zones\0[2700]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter[*]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones[securitysafe]
  Queries value:            HKCU\software\microsoft\internet explorer\main[noprotectedmodebanner]
  Queries value:            HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
  Queries value:            HKLM\software\microsoft\ctf[enableanchorcontext]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe[*]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[2106]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings\zones\0[2106]
  Queries value:            HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
  Queries value:            HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
  Queries value:            HKCU\software\microsoft\internet explorer\ietld[ietldversionlow]
  Queries value:            HKCU\software\microsoft\internet explorer\ietld[ietldversionhigh]
  Queries value:            HKLM\software\policies\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
  Queries value:            HKCU\software\policies\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
```

```
settings[cointernetcombineiuricachesize]
   Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_shim_mshelp_combine[83497c45d30bcb551f5f55f3f63b6fa1.exe]
   Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_shim_mshelp_combine[*]
   Queries value:              HKLM\software\microsoft\tracing[enableconsoletracing]
   Queries value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasapi32[enablefiletracing]
   Queries value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasapi32[filetracingmask]
   Queries value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasapi32[enableconsoletracing]
   Queries value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasapi32[consoletracingmask]
   Queries value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasapi32[maxfilesize]
   Queries value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasapi32[filedirectory]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
   Queries value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasmancs[enablefiletracing]
   Queries value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasmancs[filetracingmask]
   Queries value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasmancs[enableconsoletracing]
   Queries value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasmancs[consoletracingmask]
   Queries value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasmancs[maxfilesize]
   Queries value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasmancs[filedirectory]
   Queries value:              HKLM\software\microsoft\sqmclient\windows\disabledprocesses[b798a23b]
   Queries value:              HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
   Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
   Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
   Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxysettingsperuser]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigcustomua]
   Queries value:              HKCR\autoproxytypes\application/x-internet-signup[dllfile]
   Queries value:              HKCR\autoproxytypes\application/x-internet-signup[fileextensions]
   Queries value:              HKCR\autoproxytypes\application/x-internet-signup[default]
   Queries value:              HKCR\autoproxytypes\application/x-internet-signup[flags]
   Queries value:              HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[dllfile]
   Queries value:              HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[fileextensions]
   Queries value:              HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[default]
   Queries value:              HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[flags]
   Queries value:              HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
```

```
   Queries value:              HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
   Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
   Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
   Queries value:              HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
   Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
   Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
   Queries value:              HKLM\system\currentcontrolset\services\winsock\parameters[transports]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
```

```
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout]
  Queries value:            HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
  Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping]
  Queries value:            HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched[winsock 2.0 provider id]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
  Queries value:            HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
  Queries value:            HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6[winsock 2.0 provider id]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache[shutdownonidle]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[searchlist]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet settings\url
history[daystokeep]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2700]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[compatible]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[compatible]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet settings[user
agent]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[*]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[83497c45d30bcb551f5f55f3f63b6fa1.exe]
```

```
 Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[*]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[enabledhcp]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registrationenabled]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registeradaptername]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[domain]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpdomain]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpv6domain]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[nameserver]
 Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableutf8]
 Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
 Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
 Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
 Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[nameserver]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpnameserver]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[enabledhcp]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[registrationenabled]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[registeradaptername]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[domain]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[dhcpdomain]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[nameserver]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[dhcpnameserver]
 Queries value:              HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[queryadaptername]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[disableadapterdomainname]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registrationmaxaddresscount]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[maxnumberofaddressestoregister]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[enablemulticast]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[queryadaptername]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[disableadapterdomainname]
 Queries value:
```

```
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[disabledynamicupdate]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[enableadapterdomainnameregistration]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[registrationmaxaddresscount]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[maxnumberofaddressestoregister]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[enablemulticast]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
  Queries value:            HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}[]
  Queries value:            HKCR\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\inprocserver32[]
  Queries value:            HKCR\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprocserver32[threadingmodel]
  Queries value:            HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Queries value:            HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}[]
  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\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
  Queries value:            HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries value:            HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  Queries value:            HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
  Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
  Queries value:            HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
  Queries value:            HKLM\software\microsoft\cryptography[machineguid]
  Queries value:            HKCR\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32[]
  Queries value:            HKLM\software\microsoft\rpc\extensions[remoterpcdll]
  Queries value:            HKCR\interface\{d0074ffd-570f-4a9b-8d69-199fdba5723b}\proxystubclsid32[]
  Queries value:            HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}[]
  Queries value:            HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprocserver32[]
  Queries value:            HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32[threadingmodel]
  Queries value:            HKCR\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406}\proxystubclsid32[]
  Queries value:            HKCR\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}\proxystubclsid32[]
  Queries value:            HKCR\interface\{55272a00-42cb-11ce-8135-00aa004bb851}\proxystubclsid32[]
  Queries value:            HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}[]
  Queries value:            HKCR\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprocserver32[]
  Queries value:            HKCR\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32[threadingmodel]
  Queries value:            HKCR\interface\{bcd1de7e-2db1-418b-b047-4a74e101f8c1}\proxystubclsid32[]
  Queries value:            HKCR\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}\proxystubclsid32[]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\wpad[wpadlastnetwork]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[autoproxydetecttype]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_legacy_compression[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_legacy_compression[*]
  Queries value:            HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}[]
  Queries value:            HKCR\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32[]
  Queries value:            HKCR\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32[threadingmodel]
  Queries value:            HKLM\software\policies\microsoft\windows\currentversion\internet
settings[warnonintranet]
  Queries value:            HKCU\software\policies\microsoft\windows\currentversion\internet
settings[warnonintranet]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[warnonintranet]
  Queries value:            HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[]
  Queries value:            HKCR\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32[]
  Queries value:            HKCR\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[threadingmodel]
```

```
  Queries value:            HKCU\software\microsoft\internet explorer\recovery[autorecover]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[2000]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings\zones\0[2000]
  Queries value:            HKLM\software\microsoft\internet explorer\feed discovery[sound]
  Queries value:            HKCU\software\microsoft\ftp[use web based ftp]
  Queries value:            HKLM\system\currentcontrolset\services\netbt\linkage[export]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1a10]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[{a8a88c49-5eb2-4990-a1a2-0876022c854f}]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[privacyadvanced]
  Queries value:            HKCR\mime\database\content type\text/html[extension]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown[*]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{228d30c5-2af6-45b6-bf55-65a88ac6a29a}[wpaddecision]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{228d30c5-2af6-45b6-bf55-65a88ac6a29a}[wpaddecisiontime]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\wpad[wpadexpirationdays]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{228d30c5-2af6-45b6-bf55-65a88ac6a29a}[wpaddecisionreason]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[privdiscuishown]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1400]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_script[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_script[*]
  Queries value:            HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\progid[]
  Queries value:            HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}[]
  Queries value:            HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32[]
  Queries value:            HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[threadingmodel]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1201]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_windowedselectcontrol[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_windowedselectcontrol[*]
  Queries value:            HKCU\software\microsoft\windows script\settings[jitdebug]
  Queries value:            HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}[]
  Queries value:            HKCR\clsid\{3050f391-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
  Queries value:            HKCR\clsid\{3050f391-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
  Queries value:            HKLM\software\microsoft\internet explorer\abouturls[blank]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_about_protocol_ie7[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_about_protocol_ie7[*]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img[83497c45d30bcb551f5f55f3f63b6fa1.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img[*]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
  Queries value:            HKLM\software\microsoft\windows
```

```
nt\currentversion\languagepack\surrogatefallback[plane8]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
  Queries value:              HKLM\software\microsoft\internet explorer\main[maxrenderline]
  Queries value:              HKCR\mime\database\content type\image/jpeg[extension]
  Queries value:              HKCU\software\microsoft\internet
explorer\services[selectionactivitybuttondisable]
  Queries value:              HKCU\software\microsoft\internet explorer\suggested sites[enabled]
  Sets/Creates value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasapi32[enablefiletracing]
  Sets/Creates value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasapi32[enableconsoletracing]
  Sets/Creates value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasapi32[filetracingmask]
  Sets/Creates value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasapi32[consoletracingmask]
  Sets/Creates value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasapi32[maxfilesize]
  Sets/Creates value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasapi32[filedirectory]
  Sets/Creates value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasmancs[enablefiletracing]
  Sets/Creates value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasmancs[enableconsoletracing]
  Sets/Creates value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasmancs[filetracingmask]
  Sets/Creates value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasmancs[consoletracingmask]
  Sets/Creates value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasmancs[maxfilesize]
  Sets/Creates value:
HKLM\software\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasmancs[filedirectory]
  Sets/Creates value:         HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{228d30c5-2af6-45b6-bf55-65a88ac6a29a}[wpaddecisionreason]
  Sets/Creates value:         HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{228d30c5-2af6-45b6-bf55-65a88ac6a29a}[wpaddecisiontime]
  Sets/Creates value:         HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{228d30c5-2af6-45b6-bf55-65a88ac6a29a}[wpaddecision]
  Sets/Creates value:         HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{228d30c5-2af6-45b6-bf55-65a88ac6a29a}[wpadnetworkname]
  Sets/Creates value:         HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\a2-98-d5-56-33-71[wpaddecisionreason]
  Sets/Creates value:         HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\a2-98-d5-56-33-71[wpaddecisiontime]
  Sets/Creates value:         HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\a2-98-d5-56-33-71[wpaddecision]
  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[proxyenable]
  Value changes:              HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
  Value changes:              HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
  Value changes:              HKCU\software\microsoft\windows\currentversion\internet
settings\wpad[wpadlastnetwork]
  Value changes:              HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{228d30c5-2af6-45b6-bf55-65a88ac6a29a}[wpaddecisionreason]
  Value changes:              HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{228d30c5-2af6-45b6-bf55-65a88ac6a29a}[wpaddecisiontime]
  Value changes:              HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{228d30c5-2af6-45b6-bf55-65a88ac6a29a}[wpaddecision]
  Value changes:              HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{228d30c5-2af6-45b6-bf55-65a88ac6a29a}[wpadnetworkname]
  Value changes:              HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\a2-98-d5-56-33-71[wpaddecisionreason]
  Value changes:              HKCU\software\microsoft\windows\currentversion\internet
```

```
settings\wpad\a2-98-d5-56-33-71[wpaddecisiontime]
  Value changes:              HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\a2-98-d5-56-33-71[wpaddecision]
```