Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	206
Risk Level:	7
Date Processed:	2016-04-22 06:01:56 (UTC)
Processing Time:	61.21 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\1af5338669efabe0a9841478396871b1.exe"
Sample ID:	54
Type:	basic
Owner:	admin
Label:	1af5338669efabe0a9841478396871b1
Date Added:	2016-04-22 06:01:55 (UTC)
File Type:	PE32:win32:gui
File Size:	939520 bytes
MD5:	1af5338669efabe0a9841478396871b1
SHA256:	98511820966946e5c2c543c720816047a808816f674bc8525016f362785c8b3e
Description:	None

Pattern Matching Results

7 Creates malicious events: FakeIE [PUA , Downware]
2 ECMA Script
3 Connects to local host
5 JavaScript: Writes a string of text to a document stream
4 JavaScript: Eval method
3 HTTP connection - response code 200 (success)
3 Long sleep detected
4 Checks whether debugger is present
2 HTML file
1 YARA score 1

Static Events

YARA rule hit:	SWF
YARA rule hit:	Nonexecutable

Process/Thread Events

Creates process:	C:\windows\temp\1af5338669efabe0a9841478396871b1.exe ["C:\windows\temp\1af5338669efabe0a9841478396871b1.exe"]
Calls function:	jscript.dll:eval
Calls function:	mshtml.dll:document.write

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
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\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\RasPbFile
Creates mutex:	\Sessions\1\BaseNamedObjects\IESQMMUTEX_0_208
Creates mutex:	\Sessions\1\BaseNamedObjects\!PrivacIE!SharedMemory!Mutex
Creates mutex:	\Sessions\1\BaseNamedObjects\__DDrawExclMode__
Creates mutex:	\Sessions\1\BaseNamedObjects\__DDrawCheckExclMode__
Creates mutex:	\Sessions\1\BaseNamedObjects\DDrawWindowListMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\DDrawDriverObjectListMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\DirectSound DllMain mutex (0x000008B0)
Creates mutex:	\Sessions\1\BaseNamedObjects\{1B655094-FE2A-433c-A877-FF9793445069}
Creates mutex:	\Sessions\1\BaseNamedObjects\http://www.baidu.com/
Creates mutex:	\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!internet explorer!domstore!
Creates mutex:	\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!roaming!microsoft!internet explorer!userdata!
Creates mutex:	\Sessions\1\BaseNamedObjects\InternetExplorerDOMStoreQuota

```
  Creates mutex:            \Sessions\1\BaseNamedObjects\MSIMGSIZECacheMutex
  Creates mutex:            \Sessions\1\BaseNamedObjects\_!SHMSFTHISTORY!_
  Creates mutex:
\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!history!history.ie5!mshist012016042220160423!
  Creates event:            \KernelObjects\MaximumCommitCondition
  Creates event:            \Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1
  Creates event:            \Security\LSA_AUTHENTICATION_INITIALIZED
  Creates event:            \BaseNamedObjects\SvcctrlStartEvent_A3752DX
  Creates event:            \BaseNamedObjects\BFE_Notify_Event_{f5c68d00-9867-462b-8ad1-
67dd82817101}
  Creates event:            \Sessions\1\BaseNamedObjects\DINPUTWINMM
```

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\Roaming\Microsoft\Windows\Cookies\admin@baidu[1].txt
  Creates:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[2].txt
  Creates:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\index[1].php
  Creates:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\bd_logo1[1].png
  Creates:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\jquery-1.10.2.min_f2fb5194[1].js
  Creates:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\baidu_jgylogo3[1].gif
  Creates:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\zbios_62c636fe[1].png
  Creates:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\nuomi_510f7472[1].png
  Creates:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\icons_0e814c16[1].png
  Creates:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\all_async_search_641293e1[1].js
  Creates:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\every_cookie_aa168cb4[1].js
  Creates:                  C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\6K541L89\www.baidu[1].xml
  Creates:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[1].txt
  Creates:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[2].txt
  Creates:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WG2VLW5Y\quickdelete_9c14b01a[1].png
  Creates:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WG2VLW5Y\nu_instant_search_ebeb5baa[1].js
  Creates:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\env_beb83b45[1].swf
  Creates:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\bdsug_async_dac7ea02[1].js
  Creates:                  C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\UserData
  Creates:                  C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\index.dat
  Creates:                  C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\Y0GL1THK
  Creates:                  C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\09XN329K
  Creates:                  C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\UB8D11YC
  Creates:                  C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\73C6DRQW
  Creates:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\baiduia_b45d552b[1].js
  Creates:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com
  Creates:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
  Creates:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sxx
  Creates:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com
  Creates:                  C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
  Creates:                  C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\Y0GL1THK\userDataBIDUPSID[1].xml
  Creates:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\JSocket_9a52fc3e[1].swf
```

```
  Creates:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\error[1].htm
  Creates:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\union[1].gif
  Creates:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches
  Creates:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042220160423
  Creates:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042220160423\index.dat
  Creates:                 C:\Users\Admin\Favorites
  Creates:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\favicon[1].ico
  Creates:                 C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico
  Creates:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WG2VLW5Y\bdbri_icons_2e35e84b[1].png
  Opens:                   C:\Windows\Prefetch\1AF5338669EFABE0A984147839687-7F9632B6.pf
  Opens:                   C:\Windows\System32
  Opens:                   C:\Windows\System32\sechost.dll
  Opens:                   C:\windows\temp\1af5338669efabe0a9841478396871b1.exe.Local\
  Opens:                   C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
  Opens:                   C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
  Opens:                   C:\windows\temp\MSIMG32.dll
  Opens:                   C:\Windows\System32\msimg32.dll
  Opens:                   C:\windows\temp\VERSION.dll
  Opens:                   C:\Windows\System32\version.dll
  Opens:                   C:\Windows\System32\imm32.dll
  Opens:                   C:\Windows\WindowsShell.Manifest
  Opens:                   C:\windows\temp\msdialg100_D.dll
  Opens:                   C:\Windows\system32\msdialg100_D.dll
  Opens:                   C:\Windows\system\msdialg100_D.dll
  Opens:                   C:\Windows\msdialg100_D.dll
  Opens:                   C:\Windows\System32\Wbem\msdialg100_D.dll
  Opens:                   C:\Windows\System32\WindowsPowerShell\v1.0\msdialg100_D.dll
  Opens:                   C:\windows\temp\MFC90ENut.dll
  Opens:                   C:\Windows\system32\MFC90ENut.dll
  Opens:                   C:\Windows\system\MFC90ENut.dll
  Opens:                   C:\Windows\MFC90ENut.dll
  Opens:                   C:\Windows\System32\Wbem\MFC90ENut.dll
  Opens:                   C:\Windows\System32\WindowsPowerShell\v1.0\MFC90ENut.dll
  Opens:                   C:\windows\temp\Afx100net.dll
  Opens:                   C:\Windows\system32\Afx100net.dll
  Opens:                   C:\Windows\system\Afx100net.dll
  Opens:                   C:\Windows\Afx100net.dll
  Opens:                   C:\Windows\System32\Wbem\Afx100net.dll
  Opens:                   C:\Windows\System32\WindowsPowerShell\v1.0\Afx100net.dll
  Opens:                   C:\program files\fve31bb\zxz63d\Log.dat
  Opens:                   C:\Program Files\FVe31bb\ZXz63d\BLr11610Ho64.dll
  Opens:                   C:\Windows\System32\rpcss.dll
  Opens:                   C:\windows\temp\CRYPTBASE.dll
  Opens:                   C:\Windows\System32\cryptbase.dll
  Opens:                   C:\Windows\System32\uxtheme.dll
  Opens:                   C:\Users\Admin\AppData\Local\Temp\restart.dat
  Opens:                   C:\windows\temp\dwmapi.dll
  Opens:                   C:\Windows\System32\dwmapi.dll
  Opens:                   C:\Windows\Fonts\StaticCache.dat
  Opens:                   C:\Windows\Fonts\tahoma.ttf
  Opens:                   C:\Windows\Fonts\meiryo.ttc
  Opens:                   C:\Windows\Fonts\msgothic.ttc
  Opens:                   C:\Windows\Fonts\msjh.ttf
  Opens:                   C:\Windows\Fonts\msyh.ttf
  Opens:                   C:\Windows\Fonts\malgun.ttf
  Opens:                   C:\Windows\Fonts\mingliu.ttc
  Opens:                   C:\Windows\Fonts\simsun.ttc
  Opens:                   C:\Windows\Fonts\gulim.ttc
  Opens:                   C:\Windows\System32\en-US\user32.dll.mui
  Opens:                   C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                   C:\Windows\system32\uxtheme.dll.Config
  Opens:                   C:\program files\fve31bb\zxz63d\log.dat
  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\Temp\1af5338669efabe0a9841478396871b1.exe
  Opens:                   C:\windows\temp\ntmarta.dll
  Opens:                   C:\Windows\System32\ntmarta.dll
  Opens:                   C:\Windows\System32\en-US\urlmon.dll.mui
  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\Temp\MJPGC.TMP
  Opens:                 C:\windows\temp\SspiCli.dll
  Opens:                 C:\Windows\System32\sspicli.dll
  Opens:                 C:\Windows\System32\wininet.dll
  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
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\desktop.ini
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\desktop.ini
  Opens:                 C:\Users\Admin\AppData\Roaming
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\History
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\index.dat
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
  Opens:                 C:\windows\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:\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\MLANG.dll
  Opens:                 C:\Windows\System32\mlang.dll
  Opens:                 C:\Program Files\Common Files\microsoft shared\ink\tiptsf.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:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[1].txt
  Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[2].txt
  Opens:                 C:\Windows\System32\C_20127.NLS
  Opens:                 C:\Windows\System32\mshtml.dll
  Opens:                 C:\Windows\System32\msls31.dll
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\index[1].php
  Opens:                 C:\Windows\System32\msimtf.dll
  Opens:                 C:\Windows\System32\jscript.dll
  Opens:                 C:\Windows\System32\iepeers.dll
  Opens:                 C:\Windows\System32\winspool.drv
  Opens:                 C:\Windows\System32\dxtrans.dll
  Opens:                 C:\Windows\System32\atl.dll
  Opens:                  C:\Windows\System32\ddrawex.dll
  Opens:                  C:\Windows\System32\ddraw.dll
  Opens:                  C:\Windows\System32\dciman32.dll
  Opens:                  C:\Windows\System32\en-US\setupapi.dll.mui
  Opens:                  C:\Windows\win.ini
  Opens:                  C:\Windows\System32\en-US\ddraw.dll.mui
  Opens:                  C:\Windows\System32\dxtmsft.dll
  Opens:                  C:\windows\temp\SXS.DLL
  Opens:                  C:\Windows\System32\sxs.dll
  Opens:                  C:\Windows\Fonts\arial.ttf
  Opens:                  C:\Windows\System32\en-US\mlang.dll.mui
  Opens:                  C:\Windows\System32\C_1250.NLS
  Opens:                  C:\Windows\System32\C_1251.NLS
  Opens:                  C:\Windows\System32\C_1253.NLS
  Opens:                  C:\Windows\System32\C_1254.NLS
  Opens:                  C:\Windows\System32\C_1255.NLS
  Opens:                  C:\Windows\System32\C_1256.NLS
  Opens:                  C:\Windows\System32\C_1257.NLS
  Opens:                  C:\Windows\System32\C_1258.NLS
  Opens:                  C:\Windows\System32\C_874.NLS
  Opens:                  C:\Windows\System32\C_932.NLS
  Opens:                  C:\Windows\System32\C_936.NLS
  Opens:                  C:\Windows\System32\C_949.NLS
  Opens:                  C:\Windows\System32\C_950.NLS
  Opens:                  C:\Windows\System32\C_1361.NLS
  Opens:                  C:\Windows\Fonts\arialbd.ttf
  Opens:                  C:\Windows\Fonts\ariali.ttf
  Opens:                  C:\Windows\System32\en-US\mshtml.dll.mui
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\jquery-1.10.2.min_f2fb5194[1].js
  Opens:                  C:\windows\temp\ImgUtil.dll
  Opens:                  C:\Windows\System32\imgutil.dll
  Opens:                  C:\Windows\System32\pngfilt.dll
  Opens:
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80
  Opens:
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
  Opens:                  C:\windows\temp\D3DIM700.DLL
  Opens:                  C:\Windows\System32\d3dim700.dll
  Opens:                  C:\Windows\System32\tzres.dll
  Opens:                  C:\Windows\System32\en-US\tzres.dll.mui
  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\X3IPB3Z1\all_async_search_641293e1[1].js
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\every_cookie_aa168cb4[1].js
  Opens:                  C:\Windows\System32\Macromed\Flash\Flash10h.ocx
  Opens:                  C:\Windows\system32\Macromed\Flash\WINMM.dll
  Opens:                  C:\Windows\System32\winmm.dll
  Opens:                  C:\Windows\system32\Macromed\Flash\DSOUND.dll
  Opens:                  C:\Windows\System32\dsound.dll
  Opens:                  C:\Windows\system32\Macromed\Flash\POWRPROF.dll
  Opens:                  C:\Windows\System32\powrprof.dll
  Opens:                  C:\Windows\system32\Macromed\Flash\mscms.dll
  Opens:                  C:\Windows\System32\mscms.dll
  Opens:                  C:\Windows\system32\Macromed\Flash\USERENV.dll
  Opens:                  C:\Windows\System32\userenv.dll
  Opens:                  C:\
  Opens:                  C:\Windows\system32\Macromed\Flash\ss.sgn
  Opens:                  C:\Windows\System32\Macromed\Flash
  Opens:                  C:\Windows\system32\Macromed\Flash\ss.cfg
  Opens:                  C:\Windows\System32\Macromed\Flash\mms.cfg
  Opens:                  C:\Windows\system32\Macromed\Flash\oem.cfg
  Opens:                  C:\Windows\system32\oem.cfg
  Opens:                  C:\Users\Admin\AppData\Roaming\Adobe\Flash Player\AssetCache
  Opens:                  C:\Users\Admin\AppData\Roaming\Adobe\Flash Player
  Opens:                  C:\Windows\System32\stdole2.tlb
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\DOMStore
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\index.dat
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\6K541L89\www.baidu[1].xml
  Opens:                  C:\windows\temp\XmlLite.dll
  Opens:                  C:\Windows\System32\xmllite.dll
  Opens:                  C:\Windows\System32\mshtml.tlb
  Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[1].txt
  Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[2].txt
  Opens:                  C:\Windows\System32\urlmon.dll
  Opens:                  C:\Windows
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
```

```
Files\Content.IE5\WG2VLW5Y\nu_instant_search_ebeb5baa[1].js
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\env_beb83b45[1].swf
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\bdsug_async_dac7ea02[1].js
  Opens:                 C:\windows\temp\MMDevAPI.DLL
  Opens:                 C:\Windows\System32\MMDevAPI.dll
  Opens:                 C:\windows\temp\PROPSYS.dll
  Opens:                 C:\Windows\System32\propsys.dll
  Opens:                 C:\Windows\System32\msxml3.dll
  Opens:                 C:\Windows\System32\msxml3r.dll
  Opens:                 C:\Windows\System32\en-US\msxml3r.dll.mui
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\UserData\
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\UserData
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\index.dat
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\Y0GL1THK
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\09XN329K
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\UB8D11YC
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\73C6DRQW
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\*.*09XN329K\desktop.ini
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\73C6DRQW\desktop.ini
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\UB8D11YC\desktop.ini
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\Y0GL1THK\desktop.ini
  Opens:                 C:\windows\temp\Secur32.dll
  Opens:                 C:\Windows\System32\secur32.dll
  Opens:                 C:\windows\temp\credssp.dll
  Opens:                 C:\Windows\System32\credssp.dll
  Opens:                 C:\Windows\System32\schannel.dll
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\baiduia_b45d552b[1].js
  Opens:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\#SharedObjects
  Opens:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player
  Opens:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL\macromedia.com\support\flashplayer\sys\settings.sol
  Opens:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL\macromedia.com\support\flashplayer\sys\
  Opens:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sol
  Opens:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com\sharedObjectBIDUPSID.sol
  Opens:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com\
  Opens:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\s1.bdstatic.com\sharedObjectBIDUPSID.sol
  Opens:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\s1.bdstatic.com\
  Opens:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sol
  Opens:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\
  Opens:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sol
  Opens:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\
  Opens:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com
  Opens:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys
  Opens:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer
  Opens:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
  Opens:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sxx
  Opens:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com
  Opens:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL
  Opens:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\Y0GL1THK\userDataBIDUPSID[1].xml
  Opens:                 C:\Program Files\Internet Explorer\ieproxy.dll
  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:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\union[1].gif
  Opens:                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\JSocket_9a52fc3e[1].swf
  Opens:                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
  Opens:                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000006.db
  Opens:                    C:\Users\desktop.ini
  Opens:                    C:\Users
  Opens:                    C:\Users\Admin\AppData
  Opens:                    C:\Users\Admin\AppData\Local\Microsoft\Windows
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042220160423\
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042220160423
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042220160423\index.dat
  Opens:                    C:\Windows\System32\en-US\shell32.dll.mui
  Opens:                    C:\Users\Admin\Favorites
  Opens:                    C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico
  Opens:                    C:\windows\temp\netmsg.dll
  Opens:                    C:\Windows\System32\netmsg.dll
  Opens:                    C:\Windows\System32\en-US\netmsg.dll.mui
  Opens:                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\favicon[1].ico
  Writes to:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[1].txt
  Writes to:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[2].txt
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\index[1].php
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\jquery-1.10.2.min_f2fb5194[1].js
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\bd_logo1[1].png
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\baidu_jgylogo3[1].gif
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\zbios_62c636fe[1].png
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\nuomi_510f7472[1].png
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\icons_0e814c16[1].png
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\all_async_search_641293e1[1].js
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\every_cookie_aa168cb4[1].js
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\6K541L89\www.baidu[1].xml
  Writes to:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[1].txt
  Writes to:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[2].txt
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WG2VLW5Y\nu_instant_search_ebeb5baa[1].js
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WG2VLW5Y\quickdelete_9c14b01a[1].png
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\env_beb83b45[1].swf
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\bdsug_async_dac7ea02[1].js
  Writes to:                C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\index.dat
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\baiduia_b45d552b[1].js
  Writes to:                C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
  Writes to:                C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sxx
  Writes to:                C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
  Writes to:                C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\Y0GL1THK\userDataBIDUPSID[1].xml
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\JSocket_9a52fc3e[1].swf
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\error[1].htm
  Writes to:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042220160423\index.dat
  Writes to:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\favicon[1].ico
  Writes to:                C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico
  Writes to:               C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WG2VLW5Y\bdbri_icons_2e35e84b[1].png
  Reads from:              C:\Windows\Fonts\StaticCache.dat
  Reads from:              C:\Windows\Temp\1af5338669efabe0a9841478396871b1.exe
  Reads from:              C:\Windows\System32\drivers\etc\hosts
  Reads from:              C:\Windows\win.ini
  Reads from:              C:\Windows\System32\dxtmsft.dll
  Reads from:              C:\Windows\System32\dxtrans.dll
  Reads from:              C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\jquery-1.10.2.min_f2fb5194[1].js
  Reads from:              C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\every_cookie_aa168cb4[1].js
  Reads from:              C:\Windows\System32\Macromed\Flash\mms.cfg
  Reads from:              C:\Windows\System32\Macromed\Flash\Flash10h.ocx
  Reads from:              C:\Windows\System32\stdole2.tlb
  Reads from:              C:\Windows\System32\iepeers.dll
  Reads from:              C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\all_async_search_641293e1[1].js
  Reads from:              C:\Windows\System32\mshtml.tlb
  Reads from:              C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WG2VLW5Y\nu_instant_search_ebeb5baa[1].js
  Reads from:              C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\env_beb83b45[1].swf
  Reads from:              C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sol
  Reads from:              C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
  Reads from:              C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\bdsug_async_dac7ea02[1].js
  Reads from:              C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\X3IPB3Z1\baiduia_b45d552b[1].js
  Reads from:              C:\Windows\System32\ieframe.dll
  Reads from:              C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sxx
  Reads from:              C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\BX3UL1GO\JSocket_9a52fc3e[1].swf
  Reads from:              C:\Users\desktop.ini
  Reads from:              C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
  Reads from:              C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON\favicon[1].ico
  Deletes:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[1].txt
  Deletes:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[2].txt
  Deletes:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[1].txt
  Deletes:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
  Deletes:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sol
  Deletes:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sxx
  Deletes:                 C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HA2GV3VL\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
```

Network Events

```
  DNS query:               wpad
  DNS query:               www.baidu.com
  DNS query:               s1.bdstatic.com
  DNS query:               sclick.baidu.com
  DNS query:               formi.baidu.com
  DNS response:            www.a.shifen.com ⇒ 103.235.46.39
  DNS response:            wwwstatic1.gshifen.com ⇒ 103.235.44.90
  DNS response:            s.a.shifen.com ⇒ 123.125.115.95
  DNS response:            formi.baidu.com ⇒ 180.149.131.55
  DNS response:            formi.baidu.com ⇒ 61.135.169.120
  Connects to:             224.0.0.252:5355
  Connects to:             8.8.8.8:53
  Connects to:             103.235.46.39:80
  Connects to:             127.0.0.1:52894
  Connects to:             103.235.44.90:80
  Connects to:             123.125.115.95:80
  Connects to:             180.149.131.55:843
  Connects to:             180.149.131.55:8843
  Sends data to:           224.0.0.252:5355
  Sends data to:           8.8.8.8:53
  Sends data to:           127.0.0.1:52894
  Sends data to:           www.a.shifen.com:80 (103.235.46.39)
  Sends data to:           wwwstatic1.gshifen.com:80 (103.235.44.90)
  Sends data to:           s.a.shifen.com:80 (123.125.115.95)
  Receives data from:      8.8.8.8:53
  Receives data from:      127.0.0.1:52894
  Receives data from:         www.a.shifen.com:80 (103.235.46.39)
  Receives data from:         wwwstatic1.gshifen.com:80 (103.235.44.90)
  Receives data from:         s.a.shifen.com:80 (123.125.115.95)
```

Windows Registry Events

```
  Creates key:                HKCU\software\explore
  Creates key:                HKCU\software\microsoft\windows\currentversion\internet settings
  Creates key:                HKLM\software\microsoft\tracing
  Creates key:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32
  Creates key:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_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\explorer\runmru
  Creates key:                HKCU\software\microsoft\internet explorer\typedurls
  Creates key:                HKCU\software\microsoft\windows\currentversion\explorer\typedpaths
  Creates key:                HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{f33bffd9-5d26-428d-b279-f049ab6a7a40}
  Creates key:                HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{f33bffd9-5d26-428d-b279-f049ab6a7a40}\0a-23-64-39-4c-b7
  Creates key:                HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\0a-23-64-39-4c-b7
  Creates key:                HKCU\software\microsoft\windows\currentversion\internet
settings\p3p\history
  Creates key:                HKLM\software\microsoft\directdraw\mostrecentapplication
  Creates key:                HKCU\software\microsoft\windows script\settings
  Creates key:                HKLM\software\microsoft\direct3d\mostrecentapplication
  Creates key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata
  Creates key:                HKLM\system\currentcontrolset\control\securityproviders\schannel
  Creates key:                HKCU\software\microsoft\internet explorer\domstorage\total
  Creates key:                HKCU\software\microsoft\internet explorer\domstorage\baidu.com
  Creates key:                HKCU\software\macromedia\flashplayer
  Creates key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042220160423
  Creates key:                HKCU\software\microsoft\internet explorer\main\windowssearch
  Creates key:                HKLM\software\microsoft\downloadmanager
  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\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:                  HKLM\software\microsoft\oleaut
  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\microsoft\internet explorer\main
  Opens key:               HKLM\software\microsoft\windows\windows error reporting\wmr
  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\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\segoe ui
  Opens key:               HKLM\system\currentcontrolset\control\cmf\config
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
  Opens key:
HKLM\software\microsoft\ctf\compatibility\1af5338669efabe0a9841478396871b1.exe
  Opens key:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\ms shell dlg
  Opens key:               HKCU\software\explore
  Opens key:               HKCU\software\classes\
  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:               HKCU\software\classes\clsid\{889d2feb-5411-4565-8998-1dd2c5261283}
  Opens key:               HKCR\clsid\{889d2feb-5411-4565-8998-1dd2c5261283}
  Opens key:               HKCU\software\policies\microsoft\windows\app management
  Opens key:               HKLM\software\policies\microsoft\windows\app management
  Opens key:               HKCU\software\classes\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}
  Opens key:               HKCR\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}
  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\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\featurecontrol\feature_use_ietldlist_for_domain_determination
  Opens key:               HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
  Opens key:               HKLM\system\currentcontrolset\control\lsa\accessproviders
  Opens key:               HKLM\system\currentcontrolset\services\ldap
  Opens key:               HKCU\software\microsoft\internet explorer\ietld
  Opens key:               HKLM\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:                HKCU\software\microsoft\windows\currentversion\policies\explorer
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\1af5338669efabe0a9841478396871b1.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\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:                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\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\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:
HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings
  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\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}\propertybag
  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\024bd1a1
  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\tracing\1af5338669efabe0a9841478396871b1_rasapi32
   Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist
   Opens key:                HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
   Opens key:                HKLM\software\microsoft\sqmclient\windows\disabledsessions\
   Opens key:                HKU\
   Opens key:                HKLM\system\currentcontrolset\control\sqmservicelist
   Opens key:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs
   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\windows nt\dnsclient\dnspolicyconfig
   Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
   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\classes\protocols\name-space handler\
   Opens key:                HKCR\protocols\name-space handler
   Opens key:                HKCU\software\classes\protocols\name-space handler\http\
   Opens key:                HKCR\protocols\name-space handler\http
   Opens key:                HKCU\software\classes\protocols\name-space handler\*\
  Opens key:              HKCR\protocols\name-space handler\*
  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\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_browser_emulation
  Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
  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\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\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
  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\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:              HKCU\software\microsoft\internet explorer\international
  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\protocols\name-space handler
  Opens key:              HKCU\software\microsoft\windows\currentversion\explorer\travellog
  Opens key:              HKLM\software\microsoft\windows\currentversion\explorer\travellog
  Opens key:
HKCU\software\policies\microsoft\windows\currentversion\explorer\autocomplete
  Opens key:              HKCU\software\microsoft\windows\currentversion\explorer\autocomplete
  Opens key:
HKLM\software\policies\microsoft\windows\currentversion\explorer\autocomplete
  Opens key:              HKLM\software\microsoft\windows\currentversion\explorer\autocomplete
  Opens key:              HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}
  Opens key:              HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}
  Opens key:              HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\treatas
  Opens key:              HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\treatas
  Opens key:                HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\progid
  Opens key:                HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\progid
  Opens key:                HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
  Opens key:                HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprochandler32
  Opens key:                HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprochandler
  Opens key:                HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandler
  Opens key:                HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}
  Opens key:                HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}
  Opens key:                HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\treatas
  Opens key:                HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\treatas
  Opens key:                HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\progid
  Opens key:                HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\progid
  Opens key:                HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprocserver32
  Opens key:                HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprochandler32
  Opens key:                HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprochandler
  Opens key:                HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprochandler
  Opens key:                HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}
  Opens key:                HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}
  Opens key:                HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\treatas
  Opens key:                HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\treatas
  Opens key:                HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\progid
  Opens key:                HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\progid
  Opens key:                HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
  Opens key:                HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprochandler32
  Opens key:                HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprochandler
  Opens key:                HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprochandler
  Opens key:                HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}
  Opens key:                HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}
  Opens key:                HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\treatas
  Opens key:                HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treatas
  Opens key:                HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\progid
  Opens key:                HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\progid
  Opens key:                HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
  Opens key:                HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprochandler32
  Opens key:                HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprochandler
  Opens key:                HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandler
  Opens key:                HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32
  Opens key:                HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\autocomplete\client\
  Opens key:                HKCU\software\classes\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}
  Opens key:                HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}
  Opens key:                HKCU\software\classes\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\treatas
  Opens key:                HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treatas
  Opens key:                HKCU\software\classes\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\progid
  Opens key:                HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\progid
  Opens key:                HKCU\software\classes\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32
  Opens key:                HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprochandler32
  Opens key:                HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprochandler
  Opens key:                 HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\inprochandler
  Opens key:                 HKLM\software\microsoft\rpc\extensions
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\advanced
  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:
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:                 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\1af5338669efabe0a9841478396871b1.exe
  Opens key:                 HKCR\appid\1af5338669efabe0a9841478396871b1.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\{f33bffd9-5d26-428d-b279-f049ab6a7a40}
  Opens key:                HKLM\system\currentcontrolset\services\netbt\linkage
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\p3p\history\baidu.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\classes\protocols\filter\text/html
  Opens key:                HKCR\protocols\filter\text/html
  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\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_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:              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:              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_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:              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:              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_xssfilter
  Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter
  Opens key:              HKCU\software\microsoft\windows\currentversion\internet settings\zones
  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:              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_sslux
  Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_sslux
  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_subdownload_lockdown
  Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown
  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:              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:              HKLM\software\policies\microsoft\internet explorer\recovery
  Opens key:              HKCU\software\microsoft\internet explorer\recovery
  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:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_behaviors
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_behaviors
  Opens key:                 HKLM\software\microsoft\internet explorer\default behaviors
  Opens key:                 HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:                 HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:                 HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\treatas
  Opens key:                 HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\treatas
  Opens key:                 HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\progid
  Opens key:                 HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\progid
  Opens key:                 HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
  Opens key:                 HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
  Opens key:                 HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
  Opens key:                 HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32
  Opens key:                 HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler
  Opens key:                 HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprochandler
  Opens key:                 HKCU\software\policies\microsoft\internet explorer\persistence
  Opens key:                 HKLM\software\policies\microsoft\internet explorer\persistence
  Opens key:                 HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}
  Opens key:                 HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}
  Opens key:                 HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\treatas
  Opens key:                 HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\treatas
  Opens key:                 HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\progid
  Opens key:                 HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\progid
  Opens key:                 HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserver32
  Opens key:                 HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32
  Opens key:                 HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprochandler32
  Opens key:                 HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprochandler32
  Opens key:                 HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprochandler
  Opens key:                 HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprochandler
  Opens key:                 HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}
  Opens key:                 HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}
  Opens key:                 HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\treatas
  Opens key:                 HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\treatas
  Opens key:                 HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\progid
  Opens key:                 HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\progid
  Opens key:                 HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprocserver32
  Opens key:                 HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserver32
  Opens key:                 HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprochandler32
  Opens key:                 HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprochandler32
  Opens key:                 HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprochandler
  Opens key:                 HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprochandler
  Opens key:                 HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}
  Opens key:                 HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}
  Opens key:                 HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\treatas
  Opens key:                 HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\treatas
  Opens key:                 HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\progid
  Opens key:                 HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\progid
  Opens key:                 HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocserver32
  Opens key:                 HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32
  Opens key:                 HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprochandler32
  Opens key:                 HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprochandler32
  Opens key:                 HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprochandler
  Opens key:                 HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprochandler
  Opens key:                 HKLM\software\microsoft\windows\currentversion\setup
  Opens key:                 HKLM\software\microsoft\windows\currentversion
  Opens key:                 HKLM\hardware\devicemap\video
```

```
   Opens key:                 HKLM\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000
   Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_80ee&dev_beef&subsys_00000000&rev_00\3&267a616a&0&10
   Opens key:                 HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
9dd4432fa2e9}\0000
   Opens key:                 HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000
   Opens key:                 HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
8ed0c8eb59a8}\0000
   Opens key:                 HKLM\software\microsoft\directdraw\compatibility
   Opens key:                 HKLM\software\microsoft\directdraw\compatibility\bug!
   Opens key:                 HKLM\software\microsoft\directdraw\compatibility\demolitionderby2
   Opens key:                 HKLM\software\microsoft\directdraw\compatibility\diablo
   Opens key:                 HKLM\software\microsoft\directdraw\compatibility\mortalkombat3
   Opens key:                 HKLM\software\microsoft\directdraw\compatibility\msgolf98
   Opens key:                 HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay
   Opens key:                 HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo
   Opens key:                 HKLM\software\microsoft\directdraw\compatibility\rogue squadron
   Opens key:                 HKLM\software\microsoft\directdraw\compatibility\savage
   Opens key:                 HKLM\software\microsoft\directdraw\compatibility\scorchedplanet
   Opens key:                 HKLM\software\microsoft\directdraw\compatibility\silentthunder
   Opens key:                 HKLM\software\microsoft\directdraw\compatibility\starcraft100
   Opens key:                 HKLM\software\microsoft\directdraw\compatibility\starcraft115
   Opens key:                 HKLM\software\microsoft\directdraw\compatibility\starcraftdemo
   Opens key:                 HKLM\software\microsoft\directdraw\compatibility\terracide
   Opens key:                 HKLM\software\microsoft\directdraw\compatibility\thirddimension
   Opens key:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark
   Opens key:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark
   Opens key:                 HKLM\software\microsoft\directdraw\gammacalibrator
   Opens key:                 HKLM\software\microsoft\directdraw
   Opens key:                 HKLM\software\microsoft\direct3d
   Opens key:                 HKLM\software\microsoft\windows nt\currentversion\msasn1
   Opens key:                 HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}
   Opens key:                 HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}
   Opens key:                 HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\treatas
   Opens key:                 HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\treatas
   Opens key:                 HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\progid
   Opens key:                 HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\progid
   Opens key:                 HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserver32
   Opens key:                 HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32
   Opens key:                 HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprochandler32
   Opens key:                 HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprochandler32
   Opens key:                 HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprochandler
   Opens key:                 HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprochandler
   Opens key:                 HKCU\software\classes\dximagetransform.microsoft.shadow
   Opens key:                 HKCR\dximagetransform.microsoft.shadow
   Opens key:                 HKCU\software\classes\dximagetransform.microsoft.shadow\clsid
   Opens key:                 HKCR\dximagetransform.microsoft.shadow\clsid
   Opens key:                 HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}
   Opens key:                 HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}
   Opens key:                 HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\treatas
   Opens key:                 HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\treatas
   Opens key:                 HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\progid
   Opens key:                 HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\progid
   Opens key:                 HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\inprocserver32
   Opens key:                 HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprocserver32
   Opens key:                 HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\inprochandler32
   Opens key:                 HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprochandler32
   Opens key:                 HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\inprochandler
   Opens key:                 HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprochandler
   Opens key:                 HKLM\software\microsoft\internet explorer\activex compatibility
   Opens key:                 HKLM\software\microsoft\internet explorer\activex
compatibility\{e71b4063-3e59-11d2-952a-00c04fa34f05}
   Opens key:                 HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}
   Opens key:                 HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}
   Opens key:                 HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\treatas
   Opens key:                 HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\treatas
   Opens key:                 HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\progid
```

```
  Opens key:                  HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\progid
  Opens key:                  HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserver32
  Opens key:                  HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32
  Opens key:                  HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprochandler32
  Opens key:                  HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprochandler32
  Opens key:                  HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprochandler
  Opens key:                  HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprochandler
  Opens key:                  HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}
  Opens key:                  HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}
  Opens key:                  HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\treatas
  Opens key:                  HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\treatas
  Opens key:                  HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\progid
  Opens key:                  HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\progid
  Opens key:                  HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprocserver32
  Opens key:                  HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32
  Opens key:                  HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprochandler32
  Opens key:                  HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprochandler32
  Opens key:                  HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprochandler
  Opens key:                  HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprochandler
  Opens key:                  HKCU\software\classes\typelib
  Opens key:                  HKCR\typelib
  Opens key:                  HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}
  Opens key:                  HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}
  Opens key:                  HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1
  Opens key:                  HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1
  Opens key:                  HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
00aa003b6061}\1.1\409
  Opens key:                  HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\409
  Opens key:                  HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
00aa003b6061}\1.1\9
  Opens key:                  HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\9
  Opens key:                  HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
00aa003b6061}\1.1\0
  Opens key:                  HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0
  Opens key:                  HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
00aa003b6061}\1.1\0\win32
  Opens key:                  HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0\win32
  Opens key:                  HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}
  Opens key:                  HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}
  Opens key:                  HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1
  Opens key:                  HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1
  Opens key:                  HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
0000f87557db}\1.1\409
  Opens key:                  HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\409
  Opens key:                  HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
0000f87557db}\1.1\9
  Opens key:                  HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\9
  Opens key:                  HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
0000f87557db}\1.1\0
  Opens key:                  HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0
  Opens key:                  HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
0000f87557db}\1.1\0\win32
  Opens key:                  HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32
  Opens key:                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_behaviors_draw_reentrancy
  Opens key:                  HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_behaviors_draw_reentrancy
  Opens key:                  HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}
  Opens key:                  HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}
  Opens key:                  HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\treatas
  Opens key:                  HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\treatas
  Opens key:                  HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\progid
  Opens key:                  HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\progid
  Opens key:                  HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32
  Opens key:                  HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32
  Opens key:                  HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprochandler32
  Opens key:                  HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprochandler32
  Opens key:                  HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprochandler
  Opens key:                  HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprochandler
  Opens key:                  HKCU\software\microsoft\internet explorer\international\scripts\26
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun
  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:                HKCU\software\classes\mime\database\content type\image/png
  Opens key:                HKCR\mime\database\content type\image/png
  Opens key:                HKCU\software\classes\mime\database\content type\application/javascript
  Opens key:                HKCR\mime\database\content type\application/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\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}
  Opens key:                HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}
  Opens key:                HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\treatas
  Opens key:                HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\treatas
  Opens key:                HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\progid
  Opens key:                HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\progid
  Opens key:                HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32
  Opens key:                HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprochandler32
  Opens key:                HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprochandler
  Opens key:                HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandler
  Opens key:                HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}
  Opens key:                HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}
  Opens key:                HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\treatas
  Opens key:                HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\treatas
  Opens key:                HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\progid
  Opens key:                HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\progid
  Opens key:                HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32
  Opens key:                HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprochandler32
  Opens key:                HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprochandler
  Opens key:                HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandler
  Opens key:                HKCU\software\classes\mime\database\content type
  Opens key:                HKCR\mime\database\content type
  Opens key:                HKCU\software\classes\mime\database\content type\image/bmp\bits
  Opens key:                HKCR\mime\database\content type\image/bmp\bits
  Opens key:                HKCU\software\classes\mime\database\content type\image/gif\bits
  Opens key:                HKCR\mime\database\content type\image/gif\bits
  Opens key:                HKCU\software\classes\mime\database\content type\image/jpeg\bits
  Opens key:                HKCR\mime\database\content type\image/jpeg\bits
  Opens key:                HKCU\software\classes\mime\database\content type\image/pjpeg\bits
  Opens key:                HKCR\mime\database\content type\image/pjpeg\bits
  Opens key:                HKCU\software\classes\mime\database\content type\image/png\bits
  Opens key:                HKCR\mime\database\content type\image/png\bits
  Opens key:                HKCU\software\classes\mime\database\content type\image/tiff\bits
  Opens key:                HKCR\mime\database\content type\image/tiff\bits
  Opens key:                HKCU\software\classes\mime\database\content type\image/x-icon\bits
  Opens key:                HKCR\mime\database\content type\image/x-icon\bits
  Opens key:                HKCU\software\classes\mime\database\content type\image/x-jg\bits
  Opens key:                HKCR\mime\database\content type\image/x-jg\bits
  Opens key:                HKCU\software\classes\mime\database\content type\image/x-png\bits
  Opens key:                HKCR\mime\database\content type\image/x-png\bits
  Opens key:                HKCU\software\classes\mime\database\content type\image/x-wmf\bits
  Opens key:                HKCR\mime\database\content type\image/x-wmf\bits
  Opens key:                HKCU\software\classes\mime\database\content type\image/x-png
  Opens key:                HKCR\mime\database\content type\image/x-png
  Opens key:                HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}
  Opens key:                HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}
  Opens key:                HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\treatas
  Opens key:                HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\treatas
  Opens key:                HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\progid
  Opens key:                HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\progid
  Opens key:                HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32
  Opens key:                HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprochandler32
  Opens key:                HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprochandler
  Opens key:                HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandler
  Opens key:                HKCU\software\classes\mime\database\content type\image/gif
  Opens key:                HKCR\mime\database\content type\image/gif
  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\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\microsoft\internet explorer\new windows
  Opens key:                HKLM\software\microsoft\internet explorer\new windows
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_xmlhttp
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_xmlhttp
  Opens key:                HKCU\software\classes\shockwaveflash.shockwaveflash
  Opens key:                HKCR\shockwaveflash.shockwaveflash
  Opens key:                HKCU\software\classes\shockwaveflash.shockwaveflash\clsid
  Opens key:                HKCR\shockwaveflash.shockwaveflash\clsid
  Opens key:                HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}
  Opens key:                HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}
  Opens key:                HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\treatas
  Opens key:                HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\treatas
  Opens key:                HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\progid
  Opens key:                HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\progid
  Opens key:                HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprocserver32
  Opens key:                HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprochandler32
  Opens key:                HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprochandler
  Opens key:                HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprochandler
  Opens key:                HKLM\hardware\description\system\centralprocessor\0
  Opens key:                HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}
  Opens key:                HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}
  Opens key:                HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0
  Opens key:                HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0
  Opens key:                HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
444553540000}\1.0\409
  Opens key:                HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\409
  Opens key:                HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
444553540000}\1.0\9
  Opens key:                HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\9
  Opens key:                HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
444553540000}\1.0\0
  Opens key:                HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0
  Opens key:                HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-
444553540000}\1.0\0\win32
  Opens key:                HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0\win32
  Opens key:                HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}
  Opens key:                HKCR\typelib\{00020430-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}\2.0
  Opens key:                HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0
  Opens key:                HKCU\software\classes\typelib\{00020430-0000-0000-c000-
000000000046}\2.0\0
  Opens key:                HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0
  Opens key:                HKCU\software\classes\typelib\{00020430-0000-0000-c000-
000000000046}\2.0\0\win32
  Opens key:                HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32
  Opens key:                HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}
  Opens key:                HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}
  Opens key:                HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0
  Opens key:                HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0
  Opens key:                HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-
00c04fb6bfc4}\1.0\0
  Opens key:                HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0
  Opens key:                HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-
00c04fb6bfc4}\1.0\0\win32
  Opens key:                HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_domstorage
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_domstorage
  Opens key:                HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
  Opens key:                HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
  Opens key:                HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\treatas
  Opens key:                HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas
  Opens key:                HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\progid
  Opens key:                HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid
  Opens key:                HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32
  Opens key:                HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler32
  Opens key:                HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler
  Opens key:                HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler
  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:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_activex_repurposedetection
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_activex_repurposedetection
  Opens key:                HKLM\software\microsoft\internet explorer\activex
compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_addon_management
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_addon_management
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_alloweddomainlist
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_alloweddomainlist
  Opens key:                HKLM\software\microsoft\internet explorer\extension
compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}
  Opens key:                HKCU\software\classes\clsid\{aaf8c6ce-f972-11d0-97eb-00aa00615333}
  Opens key:                HKCR\clsid\{aaf8c6ce-f972-11d0-97eb-00aa00615333}
  Opens key:                HKCU\software\microsoft\code store database\distribution units
  Opens key:                HKLM\software\microsoft\code store database\distribution units
  Opens key:                HKLM\software\microsoft\code store database\distribution
units\{d27cdb6e-ae6d-11cf-96b8-444553540000}
  Opens key:                HKCU\software\classes\clsid
  Opens key:                HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\availableversion
  Opens key:                HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\availableversion
  Opens key:                HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\installedversion
  Opens key:                HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\installedversion
  Opens key:                HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\appid
  Opens key:                HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\appid
  Opens key:                HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\languagecheckperiod
  Opens key:                HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\languagecheckperiod
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_consult_mime_killbit_kb905915
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_consult_mime_killbit_kb905915
  Opens key:                HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\miscstatus
  Opens key:                HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\miscstatus
  Opens key:                HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\miscstatus\1
  Opens key:                HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\miscstatus\1
  Opens key:                HKLM\software\microsoft\windows\tablet pc\
  Opens key:                HKCU\software\classes\mime\database\content type\application/x-
shockwave-flash
  Opens key:                HKCR\mime\database\content type\application/x-shockwave-flash
  Opens key:                HKCU\software\classes\protocols\filter\application/x-shockwave-flash
  Opens key:                HKCR\protocols\filter\application/x-shockwave-flash
  Opens key:                HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}
  Opens key:                HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}
  Opens key:                HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\treatas
```

```
 Opens key:                 HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\treatas
 Opens key:                 HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\progid
 Opens key:                 HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\progid
 Opens key:                 HKLM\software\microsoft\windows nt\currentversion\drivers32
 Opens key:                 HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\inprocserver32
 Opens key:                 HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprocserver32
 Opens key:                 HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\inprochandler32
 Opens key:                 HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprochandler32
 Opens key:
HKCU\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
 Opens key:                 HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\inprochandler
 Opens key:                 HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprochandler
 Opens key:                 HKCU\software\microsoft\windows\currentversion\multimedia\midimap
 Opens key:                 HKLM\software\microsoft\msxml30
 Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata
 Opens key:                 HKLM\software\microsoft\cryptography\defaults\provider types\type 001
 Opens key:                 HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli
 Opens key:                 HKLM\system\currentcontrolset\control\securityproviders
 Opens key:                 HKLM\system\currentcontrolset\control\lsa\sspicache
 Opens key:                 HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll
 Opens key:                 HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
 Opens key:                 HKCU\software\microsoft\internet explorer\domstorage\baidu.com
 Opens key:                 HKCU\software\microsoft\internet explorer\domstorage\total
 Opens key:                 HKLM\software\microsoft\windows\currentversion\policies\system
 Opens key:                 HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
 Opens key:                 HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
 Opens key:                 HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\treatas
 Opens key:                 HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\treatas
 Opens key:                 HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\progid
 Opens key:                 HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\progid
 Opens key:                 HKCU\software\classes\shockwaveflash.shockwaveflash.7
 Opens key:                 HKCR\shockwaveflash.shockwaveflash.7
 Opens key:                 HKCU\software\classes\shockwaveflash.shockwaveflash.7\clsid
 Opens key:                 HKCR\shockwaveflash.shockwaveflash.7\clsid
 Opens key:                 HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprocserver32
 Opens key:                 HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserver32
 Opens key:                 HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprochandler32
 Opens key:                 HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprochandler32
 Opens key:                 HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprochandler
 Opens key:                 HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprochandler
 Opens key:                 HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}
 Opens key:                 HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}
 Opens key:                 HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\proxystubclsid32
 Opens key:                 HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32
 Opens key:                 HKCU\software\classes\clsid\{00020424-0000-0000-c000-000000000046}
 Opens key:                 HKCR\clsid\{00020424-0000-0000-c000-000000000046}
 Opens key:                 HKCU\software\classes\clsid\{00020424-0000-0000-c000-
000000000046}\treatas
 Opens key:                 HKCR\clsid\{00020424-0000-0000-c000-000000000046}\treatas
 Opens key:                 HKCU\software\classes\clsid\{00020424-0000-0000-c000-
000000000046}\progid
 Opens key:                 HKCR\clsid\{00020424-0000-0000-c000-000000000046}\progid
 Opens key:                 HKCU\software\classes\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32
 Opens key:                 HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32
 Opens key:                 HKCU\software\classes\clsid\{00020424-0000-0000-c000-
000000000046}\inprochandler32
 Opens key:                 HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprochandler32
 Opens key:                 HKCU\software\classes\clsid\{00020424-0000-0000-c000-
000000000046}\inprochandler
 Opens key:                 HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprochandler
 Opens key:                 HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\forward
 Opens key:                 HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\forward
 Opens key:                 HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\typelib
 Opens key:                 HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib
 Opens key:                 HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
 Opens key:                 HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
 Opens key:                 HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1
 Opens key:                 HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1
 Opens key:                 HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
```

```
0000c05bae0b}\1.1\0
  Opens key:                 HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0
  Opens key:                 HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
0000c05bae0b}\1.1\0\win32
  Opens key:                 HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32
  Opens key:                 HKCU\software\classes\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:                 HKCR\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:                 HKCU\software\classes\interface\{00020400-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                 HKCR\interface\{00020400-0000-0000-c000-000000000046}\proxystubclsid32
  Opens key:                 HKCU\software\classes\clsid\{00020420-0000-0000-c000-000000000046}
  Opens key:                 HKCR\clsid\{00020420-0000-0000-c000-000000000046}
  Opens key:                 HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\treatas
  Opens key:                 HKCR\clsid\{00020420-0000-0000-c000-000000000046}\treatas
  Opens key:                 HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\progid
  Opens key:                 HKCR\clsid\{00020420-0000-0000-c000-000000000046}\progid
  Opens key:                 HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32
  Opens key:                 HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32
  Opens key:                 HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandler32
  Opens key:                 HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprochandler32
  Opens key:                 HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandler
  Opens key:                 HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprochandler
  Opens key:                 HKCU\software\classes\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}
  Opens key:                 HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}
  Opens key:                 HKCU\software\classes\interface\{6d5140c1-7436-11ce-8034-
00aa006009fa}\proxystubclsid32
  Opens key:                 HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32
  Opens key:                 HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
  Opens key:                 HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
  Opens key:                 HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\treatas
  Opens key:                 HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\treatas
  Opens key:                 HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\progid
  Opens key:                 HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\progid
  Opens key:                 HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprocserver32
  Opens key:                 HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32
  Opens key:                 HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprochandler32
  Opens key:                 HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler32
  Opens key:                 HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprochandler
  Opens key:                 HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler
  Opens key:                 HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}
  Opens key:                 HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}
  Opens key:                 HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\treatas
  Opens key:                 HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\treatas
  Opens key:                 HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\progid
  Opens key:                 HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\progid
  Opens key:                 HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprocserver32
  Opens key:                 HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprocserver32
  Opens key:                 HKCU\software\classes\interface\{00020404-0000-0000-c000-000000000046}
  Opens key:                 HKCR\interface\{00020404-0000-0000-c000-000000000046}
  Opens key:                 HKCU\software\classes\interface\{00020404-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                 HKCR\interface\{00020404-0000-0000-c000-000000000046}\proxystubclsid32
  Opens key:                 HKCU\software\classes\clsid\{00020421-0000-0000-c000-000000000046}
  Opens key:                 HKCR\clsid\{00020421-0000-0000-c000-000000000046}
  Opens key:                 HKCU\software\classes\clsid\{00020421-0000-0000-c000-
000000000046}\treatas
  Opens key:                 HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprochandler32
  Opens key:                 HKCR\clsid\{00020421-0000-0000-c000-000000000046}\treatas
  Opens key:                 HKCU\software\classes\clsid\{00020421-0000-0000-c000-
000000000046}\progid
  Opens key:                 HKCR\clsid\{00020421-0000-0000-c000-000000000046}\progid
  Opens key:                 HKCU\software\classes\clsid\{00020421-0000-0000-c000-
000000000046}\inprocserver32
  Opens key:                 HKCR\clsid\{00020421-0000-0000-c000-000000000046}\inprocserver32
  Opens key:                 HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprochandler32
  Opens key:                 HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprochandler
  Opens key:                 HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprochandler
  Opens key:                 HKCU\software\classes\clsid\{00020421-0000-0000-c000-
```

```
000000000046}\inprochandler32
  Opens key:                 HKCR\clsid\{00020421-0000-0000-c000-000000000046}\inprochandler32
  Opens key:                 HKCU\software\classes\clsid\{00020421-0000-0000-c000-
000000000046}\inprochandler
  Opens key:                 HKCR\clsid\{00020421-0000-0000-c000-000000000046}\inprochandler
  Opens key:                 HKCU\software\classes\interface\{618736e0-3c3d-11cf-810c-
00aa00389b71}\proxystubclsid32
  Opens key:                 HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid32
  Opens key:                 HKCU\software\classes\interface\{332c4425-26cb-11d0-b483-00c04fd90119}
  Opens key:                 HKCR\interface\{332c4425-26cb-11d0-b483-00c04fd90119}
  Opens key:                 HKCU\software\classes\interface\{332c4425-26cb-11d0-b483-
00c04fd90119}\proxystubclsid32
  Opens key:                 HKCR\interface\{332c4425-26cb-11d0-b483-00c04fd90119}\proxystubclsid32
  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:                 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
  Opens key:                 HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder
  Opens key:                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}\shellfolder
  Opens key:                 HKLM\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}\shellfolder
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{69d250e4-6c18-
11e3-b3bc-806e6f6e6963}\
  Opens key:                 HKCU\software\classes\drive\shellex\folderextensions
  Opens key:                 HKCR\drive\shellex\folderextensions
  Opens key:                 HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-
4442-804e-409d6c4515e9}
  Opens key:                 HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}
  Opens key:                 HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
  Opens key:                 HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
  Opens key:                 HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\treatas
  Opens key:                 HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas
  Opens key:                 HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\progid
  Opens key:                 HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid
  Opens key:                 HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32
  Opens key:                 HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32
  Opens key:                 HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler32
  Opens key:                 HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler32
  Opens key:                 HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler
  Opens key:                 HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\
  Opens key:
HKLM\software\microsoft\windows\shell\registeredapplications\urlassociations\directory\openwithprogids
  Opens key:
HKCU\software\microsoft\windows\shell\associations\urlassociations\directory
  Opens key:                 HKCU\software\classes\directory
  Opens key:                 HKCR\directory
  Opens key:                HKCU\software\classes\directory\curver
  Opens key:                HKCR\directory\curver
  Opens key:                HKCR\directory\
  Opens key:                HKCU\software\classes\directory\shellex\iconhandler
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{69d250e3-6c18-
11e3-b3bc-806e6f6e6963}\
  Opens key:                HKCR\directory\shellex\iconhandler
  Opens key:                HKCU\software\classes\folder
  Opens key:                HKCR\folder
  Opens key:                HKCU\software\classes\folder\shellex\iconhandler
  Opens key:                HKCR\folder\shellex\iconhandler
  Opens key:                HKCU\software\classes\allfilesystemobjects
  Opens key:                HKCR\allfilesystemobjects
  Opens key:                HKCU\software\classes\allfilesystemobjects\shellex\iconhandler
  Opens key:                HKCR\allfilesystemobjects\shellex\iconhandler
  Opens key:                HKCU\software\classes\directory\docobject
  Opens key:                HKCR\directory\docobject
  Opens key:                HKCU\software\classes\folder\docobject
  Opens key:                HKCR\folder\docobject
  Opens key:                HKCU\software\classes\allfilesystemobjects\docobject
  Opens key:                HKCR\allfilesystemobjects\docobject
  Opens key:                HKCU\software\classes\directory\browseinplace
  Opens key:                HKCR\directory\browseinplace
  Opens key:                HKCU\software\classes\folder\browseinplace
  Opens key:                HKCR\folder\browseinplace
  Opens key:                HKCU\software\classes\allfilesystemobjects\browseinplace
  Opens key:                HKCR\allfilesystemobjects\browseinplace
  Opens key:                HKCU\software\classes\directory\clsid
  Opens key:                HKCR\directory\clsid
  Opens key:                HKCU\software\classes\folder\clsid
  Opens key:                HKCR\folder\clsid
  Opens key:                HKCU\software\classes\allfilesystemobjects\clsid
  Opens key:                HKCR\allfilesystemobjects\clsid
  Opens key:                HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
  Opens key:                HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
  Opens key:                HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32
  Opens key:                HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\shellfolder
  Opens key:                HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\shellfolder
  Opens key:                HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\treatas
  Opens key:                HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\treatas
  Opens key:                HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\progid
  Opens key:                HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\progid
  Opens key:                HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprochandler32
  Opens key:                HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprochandler
  Opens key:                HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandler
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{ff393560-c2a7-11cf-
bff4-444553540000}
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042220160423
  Opens key:                HKCU\software\microsoft\windows\currentversion\app
paths\1af5338669efabe0a9841478396871b1.exe
  Opens key:                HKLM\software\microsoft\windows\currentversion\app
paths\1af5338669efabe0a9841478396871b1.exe
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\desktop\namespace\namecustomizations
  Opens key:                HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
  Opens key:                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
  Opens key:                HKCU\software\microsoft\internet explorer\main\windowssearch
  Opens key:                HKLM\software\policies\microsoft\internet explorer\feeds
  Opens key:                HKCU\software\microsoft\internet explorer\feeds
  Opens key:                HKLM\software\microsoft\internet explorer\feeds
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}\propertybag
  Opens key:                HKLM\software\microsoft\windows search
  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\classes\mime\database\content type\image/x-icon
  Opens key:                HKCR\mime\database\content type\image/x-icon
  Opens key:                HKCU\software\classes\protocols\filter\image/x-icon
  Opens key:                HKCR\protocols\filter\image/x-icon
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_treat_image_as_authoritative
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_treat_image_as_authoritative
  Opens key:                HKLM\software\microsoft\internet explorer\activex
compatibility\{adc6cb82-424c-11d2-952a-00c04fa34f05}
  Opens key:                HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}
  Opens key:                HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}
  Opens key:                HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-
00c04fa34f05}\treatas
  Opens key:                HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\treatas
  Opens key:                HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-
00c04fa34f05}\progid
  Opens key:                HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\progid
  Opens key:                HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-
00c04fa34f05}\inprocserver32
  Opens key:                HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-
00c04fa34f05}\inprochandler32
  Opens key:                HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-
00c04fa34f05}\inprochandler
  Opens key:                HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\inprochandler
  Opens key:                HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}
  Opens key:                HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}
  Opens key:                HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\treatas
  Opens key:                HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\treatas
  Opens key:                HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\progid
  Opens key:                HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\progid
  Opens key:                HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\inprocserver32
  Opens key:                HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\inprochandler32
  Opens key:                HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\inprochandler
  Opens key:                HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprochandler
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
  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[1af5338669efabe0a9841478396871b1]
  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\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\microsoft\windows\windows error reporting\wmr[disable]
  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\locale[00000409]
  Queries value:            HKLM\system\currentcontrolset\control\nls\language groups[1]
  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\system\currentcontrolset\control\cmf\config[system]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe
ui]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
shell dlg]
  Queries value:            HKLM\software\microsoft\ole[maximumallowedallocationsize]
  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\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\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[1af5338669efabe0a9841478396871b1.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[*]
  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:              HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
  Queries value:              HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
  Queries value:              HKCU\software\microsoft\internet explorer\ietld[ietldversionlow]
  Queries value:              HKCU\software\microsoft\internet explorer\ietld[ietldversionhigh]
  Queries value:              HKCU\software\microsoft\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\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[1af5338669efabe0a9841478396871b1.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[1af5338669efabe0a9841478396871b1.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[1af5338669efabe0a9841478396871b1.exe]
  Queries value:           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
  Queries value:           HKLM\system\currentcontrolset\control\wmi\security[0cfe0455-93ba-440d-
a3fe-553973d0b723]
  Queries value:           HKLM\system\currentcontrolset\control\wmi\security[797fabac-7b58-4796-
b924-d51178a59ce4]
  Queries value:           HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
  Queries value:           HKLM\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\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\{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\{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\{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:
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\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[1af5338669efabe0a9841478396871b1.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:           HKLM\software\microsoft\tracing[enableconsoletracing]
  Queries value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32[enablefiletracing]
  Queries value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32[filetracingmask]
  Queries value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32[enableconsoletracing]
  Queries value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32[consoletracingmask]
  Queries value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32[maxfilesize]
  Queries value:
```

```
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32[filedirectory]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
  Queries value:            HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a5ea4f8e]
  Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
  Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
  Queries value:            HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
  Queries value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs[enablefiletracing]
  Queries value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs[filetracingmask]
  Queries value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs[enableconsoletracing]
  Queries value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs[consoletracingmask]
  Queries value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs[maxfilesize]
  Queries value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs[filedirectory]
  Queries value:            HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxysettingsperuser]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigcustomua]
  Queries value:            HKCR\autoproxytypes\application/x-internet-signup[dllfile]
  Queries value:            HKCR\autoproxytypes\application/x-internet-signup[fileextensions]
  Queries value:            HKCR\autoproxytypes\application/x-internet-signup[default]
  Queries value:            HKCR\autoproxytypes\application/x-internet-signup[flags]
  Queries value:            HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[dllfile]
  Queries value:            HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[fileextensions]
  Queries value:            HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[default]
  Queries value:            HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[flags]
  Queries value:            HKLM\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\dnscache\parameters[appendtomultilabelname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
  Queries value:            HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
  Queries value:            HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
  Queries value:            HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
  Queries value:            HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout]
  Queries value:            HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
  Queries value:             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[1af5338669efabe0a9841478396871b1.exe]
  Queries value:             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[*]
  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_browser_emulation[1af5338669efabe0a9841478396871b1.exe]
  Queries value:             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation[*]
  Queries value:             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[1af5338669efabe0a9841478396871b1.exe]
  Queries value:             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[*]
  Queries value:             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[1af5338669efabe0a9841478396871b1.exe]
  Queries value:             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[*]
  Queries value:             HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
  Queries value:             HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
  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\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\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:             HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableutf8]
  Queries value:             HKCU\software\microsoft\internet explorer\international[acceptlanguage]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_legacy_compression[1af5338669efabe0a9841478396871b1.exe]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_legacy_compression[*]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[append completion]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
  Queries value:              HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}[]
  Queries value:              HKCR\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
  Queries value:              HKCR\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
  Queries value:              HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}[]
  Queries value:              HKCR\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprocserver32[]
  Queries value:              HKCR\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprocserver32[threadingmodel]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\runmru[mrulist]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\runmru[c]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\runmru[b]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\runmru[a]
  Queries value:              HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}[]
  Queries value:              HKCR\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
  Queries value:              HKCR\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
  Queries value:              HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}[]
  Queries value:              HKCR\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
  Queries value:              HKCR\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
  Queries value:              HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32[]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\autocomplete\client[]
  Queries value:              HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\progid[]
  Queries value:              HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}[]
  Queries value:              HKCR\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\inprocserver32[]
  Queries value:              HKCR\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32[threadingmodel]
  Queries value:              HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Queries value:              HKCU\control panel\desktop[smoothscroll]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewalphaselect]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[acclistviewv6]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
  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:
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:              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\session
manager[safeprocesssearchmode]
```

```
  Queries value:              HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries value:              HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  Queries value:              HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
  Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
  Queries value:              HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
  Queries value:              HKLM\software\microsoft\cryptography[machineguid]
  Queries value:              HKCR\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\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[{aeba21fa-782a-4a90-978d-b72164c80120}]
  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_mime_sniffing[1af5338669efabe0a9841478396871b1.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[1af5338669efabe0a9841478396871b1.exe]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_feeds[*]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[1af5338669efabe0a9841478396871b1.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:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[1af5338669efabe0a9841478396871b1.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[1af5338669efabe0a9841478396871b1.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[9e3b3947-ca5d-4614-
91a2-7b624e0e7244]
  Queries value:              HKLM\software\microsoft\internet explorer\application
compatibility[1af5338669efabe0a9841478396871b1.exe]
  Queries value:              HKCU\software\microsoft\internet explorer\domstorage[totallimit]
  Queries value:              HKCU\software\microsoft\internet explorer\domstorage[domainlimit]
  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[1af5338669efabe0a9841478396871b1.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[1af5338669efabe0a9841478396871b1.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\microsoft\windows\currentversion\internet settings\url
history[daystokeep]
  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:          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[1af5338669efabe0a9841478396871b1.exe]
  Queries value:          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation[*]
  Queries value:          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter[1af5338669efabe0a9841478396871b1.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\internet
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe[1af5338669efabe0a9841478396871b1.exe]
  Queries value:          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe[*]
  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_sslux[1af5338669efabe0a9841478396871b1.exe]
  Queries value:          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_sslux[*]
  Queries value:          HKLM\software\policies\microsoft\windows\currentversion\internet
settings[warnonintranet]
  Queries value:          HKCU\software\policies\microsoft\windows\currentversion\internet
settings[warnonintranet]
  Queries value:          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown[1af5338669efabe0a9841478396871b1.exe]
  Queries value:          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown[*]
  Queries value:          HKLM\software\policies\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[warnonintranet]
  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:          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:          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\internet explorer\recovery[autorecover]
  Queries value:          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img[1af5338669efabe0a9841478396871b1.exe]
  Queries value:          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img[*]
  Queries value:          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_behaviors[1af5338669efabe0a9841478396871b1.exe]
  Queries value:          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_behaviors[*]
  Queries value:          HKLM\software\microsoft\internet explorer\default behaviors[homepage]
  Queries value:          HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\progid[]
  Queries value:          HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}[]
  Queries value:          HKCR\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[inprocserver32]
  Queries value:          HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
  Queries value:          HKCR\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
  Queries value:          HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\progid[]
  Queries value:          HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}[]
  Queries value:          HKCR\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserver32[inprocserver32]
```

```
  Queries value:              HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32[]
  Queries value:              HKCR\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserver32[threadingmodel]
  Queries value:              HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}[]
  Queries value:              HKCR\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserver32[]
  Queries value:              HKCR\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprocserver32[threadingmodel]
  Queries value:              HKLM\software\microsoft\internet explorer\default
behaviors[dxtfilterbehavior]
  Queries value:              HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}[]
  Queries value:              HKCR\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32[]
  Queries value:              HKCR\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocserver32[threadingmodel]
  Queries value:              HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
  Queries value:              HKLM\software\microsoft\windows\currentversion[devicepath]
  Queries value:              HKLM\hardware\devicemap\video[maxobjectnumber]
  Queries value:              HKLM\hardware\devicemap\video[\device\video3]
  Queries value:              HKLM\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000[pruningmode]
  Queries value:              HKLM\hardware\devicemap\video[\device\video0]
  Queries value:              HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
9dd4432fa2e9}\0000[pruningmode]
  Queries value:              HKLM\hardware\devicemap\video[\device\video1]
  Queries value:              HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000[pruningmode]
  Queries value:              HKLM\hardware\devicemap\video[\device\video2]
  Queries value:              HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
8ed0c8eb59a8}\0000[pruningmode]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\bug![name]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\bug![flags]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\bug![id]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[name]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[flags]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[id]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\diablo[name]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\diablo[flags]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\diablo[id]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[name]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[flags]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[id]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\msgolf98[name]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\msgolf98[flags]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\msgolf98[id]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[name]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[flags]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[id]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[name]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[flags]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[id]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\rogue squadron[name]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\rogue squadron[flags]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\rogue squadron[id]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\savage[name]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\savage[flags]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\savage[id]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[name]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[flags]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[id]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\silentthunder[name]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\silentthunder[flags]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\silentthunder[id]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\starcraft100[name]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\starcraft100[flags]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\starcraft100[id]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\starcraft115[name]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\starcraft115[flags]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\starcraft115[id]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\starcraftdemo[name]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\starcraftdemo[flags]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\starcraftdemo[id]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\terracide[name]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\terracide[flags]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\terracide[id]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\thirddimension[name]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\thirddimension[flags]
  Queries value:              HKLM\software\microsoft\directdraw\compatibility\thirddimension[id]
  Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[name]
  Queries value:
```

```
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[flags]
  Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[id]
  Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[name]
  Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[flags]
  Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[id]
  Queries value:              HKLM\software\microsoft\directdraw[modexonly]
  Queries value:              HKLM\software\microsoft\directdraw[emulationonly]
  Queries value:              HKLM\software\microsoft\directdraw[showframerate]
  Queries value:              HKLM\software\microsoft\directdraw[enableprintscreen]
  Queries value:              HKLM\software\microsoft\directdraw[forceagpsupport]
  Queries value:              HKLM\software\microsoft\directdraw[disableagpsupport]
  Queries value:              HKLM\software\microsoft\directdraw[disablemmx]
  Queries value:              HKLM\software\microsoft\directdraw[disableddscapsinddsd]
  Queries value:              HKLM\software\microsoft\directdraw[disablewidersurfaces]
  Queries value:              HKLM\software\microsoft\directdraw[usenonlocalvidmem]
  Queries value:              HKLM\software\microsoft\directdraw[forcerefreshrate]
  Queries value:              HKLM\software\microsoft\direct3d[flipnovsync]
  Queries value:              HKLM\software\microsoft\directdraw[owndc]
  Queries value:              HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\progid[]
  Queries value:              HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}[]
  Queries value:              HKCR\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32[]
  Queries value:              HKCR\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserver32[threadingmodel]
  Queries value:              HKCR\dximagetransform.microsoft.shadow\clsid[]
  Queries value:              HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\progid[]
  Queries value:              HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}[]
  Queries value:              HKCR\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprocserver32[]
  Queries value:              HKCR\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\inprocserver32[threadingmodel]
  Queries value:              HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}[]
  Queries value:              HKCR\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32[]
  Queries value:              HKCR\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserver32[threadingmodel]
  Queries value:              HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\progid[]
  Queries value:              HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}[]
  Queries value:              HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32[]
  Queries value:              HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprocserver32[threadingmodel]
  Queries value:              HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0\win32[]
  Queries value:              HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32[]
  Queries value:              HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}[]
  Queries value:              HKCR\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32[]
  Queries value:              HKCR\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32[threadingmodel]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[1250]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[1251]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[1253]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[1254]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[1255]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[1256]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[1257]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[1258]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[874]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[932]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[936]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[949]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[1361]
  Queries value:              HKCU\software\microsoft\internet
explorer\international\scripts\26[iefontsize]
  Queries value:              HKCU\software\microsoft\internet
explorer\international\scripts\26[iefontsizeprivate]
  Queries value:              HKCU\software\microsoft\internet
explorer\international\scripts\26[iepropfontname]
  Queries value:              HKCU\software\microsoft\internet
explorer\international\scripts\26[iefixedfontname]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane1]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane2]
```

```
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane3]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane4]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane5]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane6]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane7]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane8]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane9]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane10]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane11]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane12]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane13]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane14]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane15]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane16]
  Queries value:           HKCU\software\microsoft\windows script\settings[jitdebug]
  Queries value:           HKCR\mime\database\content type\image/png[extension]
  Queries value:           HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\progid[]
  Queries value:           HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}[]
  Queries value:           HKCR\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[inprocserver32]
  Queries value:           HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[]
  Queries value:           HKCR\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[threadingmodel]
  Queries value:           HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\progid[]
  Queries value:           HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}[]
  Queries value:           HKCR\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32[inprocserver32]
  Queries value:           HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32[]
  Queries value:           HKCR\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32[threadingmodel]
  Queries value:           HKCR\mime\database\content type\image/bmp\bits[0]
  Queries value:           HKCR\mime\database\content type\image/gif\bits[0]
  Queries value:           HKCR\mime\database\content type\image/jpeg\bits[0]
  Queries value:           HKCR\mime\database\content type\image/pjpeg\bits[0]
  Queries value:           HKCR\mime\database\content type\image/png\bits[0]
  Queries value:           HKCR\mime\database\content type\image/x-png\bits[0]
  Queries value:           HKCR\mime\database\content type\image/x-wmf\bits[0]
  Queries value:           HKCR\mime\database\content type\image/x-png[image filter clsid]
  Queries value:           HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\progid[]
  Queries value:           HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}[]
  Queries value:           HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32[inprocserver32]
  Queries value:           HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[]
  Queries value:           HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32[threadingmodel]
  Queries value:           HKLM\software\microsoft\direct3d[disablemmx]
  Queries value:           HKLM\software\microsoft\direct3d[disablex3d]
  Queries value:           HKLM\software\microsoft\direct3d[fewvertices]
  Queries value:           HKLM\software\microsoft\direct3d[disablevidmemvbs]
  Queries value:           HKCR\mime\database\content type\image/gif[extension]
  Queries value:           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_script[1af5338669efabe0a9841478396871b1.exe]
  Queries value:           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_script[*]
  Queries value:           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_windowedselectcontrol[1af5338669efabe0a9841478396871b1.exe]
  Queries value:           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_windowedselectcontrol[*]
  Queries value:           HKCU\software\microsoft\internet explorer\new
windows[accuserinitonclick]
  Queries value:           HKCR\shockwaveflash.shockwaveflash\clsid[]
  Queries value:           HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\progid[]
  Queries value:           HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}[]
  Queries value:           HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprocserver32[inprocserver32]
  Queries value:           HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprocserver32[]
  Queries value:           HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-
444553540000}\inprocserver32[threadingmodel]
  Queries value:           HKLM\system\currentcontrolset\control\wmi\security[12e1ddac-7ebb-434f-
bc58-54c27d745f8f]
  Queries value:            HKLM\system\currentcontrolset\control\wmi\security[d53270e3-c8cf-4707-
958a-dad20c90073c]
  Queries value:            HKLM\hardware\description\system\centralprocessor\0[~mhz]
  Queries value:            HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0\win32[]
  Queries value:            HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32[]
  Queries value:            HKLM\software\microsoft\internet explorer\default behaviors[userdata]
  Queries value:            HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32[]
  Queries value:            HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[]
  Queries value:            HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[]
  Queries value:            HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[threadingmodel]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2000]
  Queries value:            HKLM\software\microsoft\internet explorer\feed discovery[sound]
  Queries value:            HKCU\software\microsoft\ftp[use web based ftp]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_activex_repurposedetection[1af5338669efabe0a9841478396871b1.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_activex_repurposedetection[*]
  Queries value:            HKLM\software\microsoft\internet explorer\activex
compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}[compatibility flags]
  Queries value:            HKLM\software\microsoft\internet explorer\activex
compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}[miscstatus flags]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_addon_management[1af5338669efabe0a9841478396871b1.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_addon_management[*]
  Queries value:            HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\miscstatus\1[]
  Queries value:            HKLM\software\microsoft\windows\tablet pc[istabletpc]
  Queries value:            HKCR\mime\database\content type\application/x-shockwave-flash[extension]
  Queries value:            HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\progid[]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
  Queries value:            HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}[]
  Queries value:            HKCR\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\inprocserver32[inprocserver32]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
  Queries value:            HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprocserver32[]
  Queries value:            HKCR\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\inprocserver32[threadingmodel]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
  Queries value:
HKCU\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1606]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cacherepair]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cachepath]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cacheprefix]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cachelimit]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cacheoptions]
  Queries value:            HKLM\software\microsoft\cryptography\defaults\provider types\type
001[name]
  Queries value:
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignaturedll]
  Queries value:
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignatureroutine]
  Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[name]
  Queries value:              HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[comment]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[capabilities]
  Queries value:              HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[rpcid]
  Queries value:              HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[version]
  Queries value:              HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[type]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[tokensize]
  Queries value:
HKLM\system\currentcontrolset\control\securityproviders\schannel[usercontextlockcount]
  Queries value:
HKLM\system\currentcontrolset\control\securityproviders\schannel[usercontextlistcount]
  Queries value:              HKCU\software\microsoft\internet explorer\domstorage\total[]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\system[enablelua]
  Queries value:              HKCU\software\macromedia\flashplayer[flashplayerversion]
  Queries value:              HKCU\software\microsoft\internet explorer\domstorage\baidu.com[]
  Queries value:              HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}[]
  Queries value:              HKCR\shockwaveflash.shockwaveflash.7\clsid[]
  Queries value:              HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32[]
  Queries value:              HKCR\clsid\{00020424-0000-0000-c000-000000000046}[]
  Queries value:              HKCR\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32[]
  Queries value:              HKCR\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
  Queries value:              HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib[]
  Queries value:              HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib[version]
  Queries value:              HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32[]
  Queries value:              HKLM\software\microsoft\rpc[udtalignmentpolicy]
  Queries value:              HKCR\interface\{00020400-0000-0000-c000-000000000046}\proxystubclsid32[]
  Queries value:              HKCR\clsid\{00020420-0000-0000-c000-000000000046}[]
  Queries value:              HKCR\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32[]
  Queries value:              HKCR\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
  Queries value:              HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32[]
  Queries value:              HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}[]
  Queries value:              HKCR\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[]
  Queries value:              HKCR\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprocserver32[threadingmodel]
  Queries value:              HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\progid[]
  Queries value:              HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}[]
  Queries value:              HKCR\interface\{00020404-0000-0000-c000-000000000046}\proxystubclsid32[]
  Queries value:              HKCR\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprocserver32[]
  Queries value:              HKCR\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprocserver32[threadingmodel]
  Queries value:              HKCR\clsid\{00020421-0000-0000-c000-000000000046}[]
  Queries value:              HKCR\clsid\{00020421-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{00020421-0000-0000-c000-000000000046}\inprocserver32[]
  Queries value:              HKCR\clsid\{00020421-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
  Queries value:              HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid32[]
  Queries value:              HKCR\interface\{332c4425-26cb-11d0-b483-00c04fd90119}\proxystubclsid32[]
  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:              HKCU\software\microsoft\internet
explorer\services[selectionactivitybuttondisable]
  Queries value:              HKCU\software\microsoft\internet explorer\suggested sites[enabled]
  Queries value:              HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
  Queries value:              HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[callforattributes]
  Queries value:              HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[restrictedattributes]
  Queries value:              HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsfordisplay]
  Queries value:              HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hidefolderverbs]
  Queries value:              HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[usedrophandler]
  Queries value:              HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsforparsing]
```

```
   Queries value:                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsparsedisplayname]
   Queries value:                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforoverlay]
   Queries value:                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[mapnetdriveverbs]
   Queries value:                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforinfotip]
   Queries value:                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideinwebview]
   Queries value:                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideondesktopperuser]
   Queries value:                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsaliasednotifications]
   Queries value:                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsuniversaldelegate]
   Queries value:                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[nofilefolderjunction]
   Queries value:                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[pintonamespacetree]
   Queries value:                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hasnavigationenum]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{69d250e4-6c18-
11e3-b3bc-806e6f6e6963}[data]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{69d250e4-6c18-
11e3-b3bc-806e6f6e6963}[generation]
   Queries value:                HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
   Queries value:                HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
   Queries value:                HKCR\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[inprocserver32]
   Queries value:                HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[]
   Queries value:                HKCR\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[threadingmodel]
   Queries value:                HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
   Queries value:                HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
   Queries value:                HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{69d250e3-6c18-
11e3-b3bc-806e6f6e6963}[data]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{69d250e3-6c18-
11e3-b3bc-806e6f6e6963}[generation]
   Queries value:                HKCR\directory[docobject]
   Queries value:                HKCR\folder[docobject]
   Queries value:                HKCR\allfilesystemobjects[docobject]
   Queries value:                HKCR\directory[browseinplace]
   Queries value:                HKCR\folder[browseinplace]
   Queries value:                HKCR\allfilesystemobjects[browseinplace]
   Queries value:                HKCR\directory[isshortcut]
   Queries value:                HKCR\folder[isshortcut]
   Queries value:                HKCR\allfilesystemobjects[isshortcut]
```

```
  Queries value:              HKCR\directory[alwaysshowext]
  Queries value:              HKCR\directory[nevershowext]
  Queries value:              HKCR\folder[nevershowext]
  Queries value:              HKCR\allfilesystemobjects[nevershowext]
  Queries value:              HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32[]
  Queries value:              HKCR\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32[loadwithoutcom]
  Queries value:              HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {000214e6-0000-0000-c000-000000000046}
0xffff]
  Queries value:              HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[]
  Queries value:              HKCR\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32[threadingmodel]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042220160423[cacherepair]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042220160423[cachepath]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042220160423[cacheprefix]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042220160423[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042220160423[cacheoptions]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}[]
  Queries value:              HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[localizedstring]
  Queries value:              HKCU\software\microsoft\internet
explorer\main\windowssearch[enabledscopes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[category]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[name]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[parentfolder]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[description]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[relativepath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[parsingname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[infotip]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[localizedname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[icon]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[security]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[streamresource]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[streamresourcetype]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[localredirectonly]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[roamable]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[precreate]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[stream]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[publishexpandedpath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[attributes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[foldertypeid]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-
87bd-30b759fa33dd}[initfolderhandler]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[favorites]
  Queries value:            HKLM\software\microsoft\windows search[currentversion]
  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\downloadmanager[cacheok]
  Queries value:            HKCR\mime\database\content type\image/x-icon[extension]
  Queries value:            HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\progid[]
  Queries value:            HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}[]
  Queries value:            HKCR\clsid\{adc6cb82-424c-11d2-952a-
00c04fa34f05}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\inprocserver32[]
  Queries value:            HKCR\clsid\{adc6cb82-424c-11d2-952a-
00c04fa34f05}\inprocserver32[threadingmodel]
  Queries value:            HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}[]
  Queries value:            HKCR\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32[]
  Queries value:            HKCR\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\inprocserver32[threadingmodel]
  Sets/Creates value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32[enablefiletracing]
  Sets/Creates value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32[enableconsoletracing]
  Sets/Creates value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32[filetracingmask]
  Sets/Creates value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32[consoletracingmask]
  Sets/Creates value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32[maxfilesize]
  Sets/Creates value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasapi32[filedirectory]
  Sets/Creates value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs[enablefiletracing]
  Sets/Creates value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs[enableconsoletracing]
  Sets/Creates value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs[filetracingmask]
  Sets/Creates value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs[consoletracingmask]
  Sets/Creates value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs[maxfilesize]
  Sets/Creates value:
HKLM\software\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs[filedirectory]
  Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{f33bffd9-5d26-428d-b279-f049ab6a7a40}[wpaddecisionreason]
  Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{f33bffd9-5d26-428d-b279-f049ab6a7a40}[wpaddecisiontime]
  Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{f33bffd9-5d26-428d-b279-f049ab6a7a40}[wpaddecision]
  Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{f33bffd9-5d26-428d-b279-f049ab6a7a40}[wpadnetworkname]
  Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\0a-23-64-39-4c-b7[wpaddecisionreason]
  Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\0a-23-64-39-4c-b7[wpaddecisiontime]
  Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\0a-23-64-39-4c-b7[wpaddecision]
  Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cachepath]
  Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cacheprefix]
  Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cachelimit]
  Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cacheoptions]
  Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cacherepair]
  Sets/Creates value:       HKCU\software\microsoft\internet explorer\domstorage\baidu.com[]
  Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042220160423[cachepath]
  Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\internet
```

```
settings\5.0\cache\extensible cache\mshist012016042220160423[cacheprefix]
  Sets/Creates value:        HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042220160423[cachelimit]
  Sets/Creates value:        HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042220160423[cacheoptions]
  Sets/Creates value:        HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042220160423[cacherepair]
  Value changes:             HKCU\software\microsoft\internet explorer\main[disable script debugger]
  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\{f33bffd9-5d26-428d-b279-f049ab6a7a40}[wpaddecisionreason]
  Value changes:             HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{f33bffd9-5d26-428d-b279-f049ab6a7a40}[wpaddecisiontime]
  Value changes:             HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{f33bffd9-5d26-428d-b279-f049ab6a7a40}[wpaddecision]
  Value changes:             HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{f33bffd9-5d26-428d-b279-f049ab6a7a40}[wpadnetworkname]
  Value changes:             HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\0a-23-64-39-4c-b7[wpaddecisionreason]
  Value changes:             HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\0a-23-64-39-4c-b7[wpaddecisiontime]
  Value changes:             HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\0a-23-64-39-4c-b7[wpaddecision]
  Value changes:             HKLM\software\microsoft\directdraw\mostrecentapplication[name]
  Value changes:             HKLM\software\microsoft\directdraw\mostrecentapplication[id]
  Value changes:             HKLM\software\microsoft\direct3d\mostrecentapplication[name]
  Value changes:             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cachepath]
  Value changes:             HKCU\software\microsoft\internet explorer\domstorage\total[]
  Value changes:             HKCU\software\microsoft\internet explorer\domstorage\baidu.com[]
  Value changes:             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042220160423[cachepath]
  Value changes:             HKCU\software\microsoft\internet explorer\main\windowssearch[version]
```