

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	25	Host: mag2, Sample ID: 7, Task ID: 25
Risk Level:	5	
Date Processed:	2016-04-08 09:39:52 (UTC)	
Processing Time:	61.38 seconds	
Virtual Environment:	IntelliVM	
Execution Arguments:	"c:\windows\temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe"	

Sample ID:	7
Type:	basic
Owner:	admin
Label:	62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb
Date Added:	2016-04-08 09:39:50 (UTC)
File Type:	PE32:win32:gui
File Size:	955904 bytes
MD5:	4c838f1570b3a7ff6f491e6ec1ef6895
SHA256:	62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb
Description:	None

Pattern Matching Results

- 2 ECMA Script
- 3 HTTP connection - response code 200 (success)
- 5 Possible injector
- 2 HTML file
- 5 JavaScript: Writes a string of text to a document stream
- 1 HTTP connection - response code 404 (file not found)
- 3 Connects to local host
- 1 YARA score 1
- 4 JavaScript: Eval method
- 3 Long sleep detected
- 4 Checks whether debugger is present

Static Events

YARA rule hit:	SWF
YARA rule hit:	Nonexecutable

Process/Thread Events

Creates process:	C:\windows\temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
	["C:\windows\temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.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\!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 (0x0000089C)
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\!SHMSFTHISTORY!_
Creates mutex:	\Sessions\1\BaseNamedObjects\c:\users\admin!appdata!local!microsoft!windows!history!history.ie5!mshist012016040820160409!
Creates mutex:	\Sessions\1\BaseNamedObjects\MSIMGSIzeCacheMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\c:\users\admin!appdata!roaming!microsoft!windows!ietldcache!
Creates event:	\KernelObjects\MaximumCommitCondition
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtFActivated.Default1
Creates event:	\Security\LSA_AUTHENTICATION_INITIALIZED
Creates event:	\BaseNamedObjects\Svcctrl!StartEvent_A3752DX
Creates event:	\BaseNamedObjects\BFE_Notify_Event_{22ad8c5a-3fa3-4bc7-8399-a35fa8fee727}
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\TZILKL9J\index[1].php
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\bd_logo1[1].png
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\jquery-1.10.2.min_f2fb5194[1].js
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\baidu_jgylgo3[1].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\nuomi_510f7472[1].png
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\zbios_62c636fe[1].png
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\icons_0e814c16[1].png
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\all_async_search_d0d1b2ec[1].js
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\TZILKL9J\every_cookie_aa168cb4[1].js
Creates: C:\Users\Admin\AppData\Roaming\Adobe\Flash Player
Creates: C:\Users\Admin\AppData\Roaming\Adobe\Flash Player\AssetCache
Creates: C:\Users\Admin\AppData\Roaming\Adobe\Flash Player\AssetCache\QW4AL2EV
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\quickdelete_9c14b01a[1].png
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\nu_instant_search_ebeb5baa[1].js
Creates: C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\U73CBGV\www.baidu[1].xml
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\bd sug_async_1cb857eb[1].js
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\env_beb83b45[1].swf
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\JEQSE8W1
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\2I2VAGUP
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\Mw2Q5IZ4
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\UIMZBC64
Creates: C:\Users\Admin\AppData\Roaming\Macromedia
Creates: C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player
Creates: C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\#SharedObjects
Creates: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HHYYWDWK
Creates: C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\macromedia.com
Creates: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support
Creates: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer
Creates: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys
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\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\#SharedObjects\HHYYWDWK\s1.bdstatic.com
Creates: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HHYYWDWK\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\JEQSE8W1\UserDataBIDUPSID[1].xml
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches
Creates:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016040820160409
Creates:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016040820160409\index.dat
Creates: C:\Users\Admin\Favorites
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\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\WM60WM90\baiduia_b45d552b[1].js
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\pc[1].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\ps_default[1].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\ps_default[1].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\ps_default[1].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\ps_default[1].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\ps_default[2].gif

Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\JSocket_9a52fc3e[1].swf
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\s[1].txt
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\union[1].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\ps_default[2].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\pc[1].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\u=658147196,2876094505&fm=96&s=418421F0022805031201C81C030050DB[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\u=2752145054,3166876123&fm=58[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\u=2521629668,33371966&fm=96&s=66927722A5E7DF07E68DE8D70100C0A3[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\u=4267309876,3923431364&fm=96&s=EA90E90821C392A6BCAFF10D0300E0E[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\u=2731110358,2228192387&fm=58[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\u=2719784904,580575759&fm=58[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\u=2627075135,3105681134&fm=58[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\u=2269530877,797123279&fm=96&s=FB1A4A81CFB4358A30255930300B092[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\u=2413434242,1825510918&fm=96&s=4E9241887E120FDE0C4DF0800300E081[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\u=918841094,1711827117&fm=58[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\u=2584046138,590027024&fm=96&s=4E927488A700F8ACA30D956030050E0[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\his[1]
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\u=1010662780,933723174&fm=58[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\u=3841058258,2231097427&fm=58[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\u=2916809114,3153528632&fm=96&s=1EF66984415003CA44803596030080C2[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\u=4121919617,900972282&fm=58[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\union[1].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\u=2781679007,565939595&fm=58[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\wb[1].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\ielib_0108[1].js
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\u=532204567,887570784&fm=58[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\wb[1].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\u=2177447570,2292449148&fm=82&s=21904D3064EAEF090584C9C6010070A3&w=121&h=81&img[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\u=1489011112,1613214565&fm=58[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\u=1779799337,1886987922&fm=58[1].jpg
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\wb[1].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\wb[2].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\o_0108[1].swf
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\wb[2].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\wb[2].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\wb[3].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\wb[1].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\wb[3].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\wb[3].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\wb[4].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\wb[2].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\wb[4].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\wb[4].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\wb[5].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\wb[3].gif
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\2I2VAGUP\oXMLStore[1].xml
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\wb[5].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\ps_fp[1].htm
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\wb[6].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\wb[4].gif
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\wb[6].gif

```

Opens: C:\Windows\Prefetch\62DDFBF757BE511F30B6D330963C1-E2075B81 .pf
Opens: C:\Windows
Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\System32\wow64win.dll
Opens: C:\Windows\System32\wow64cpu.dll
Opens: C:\Windows\system32\wow64log.dll
Opens: C:\Windows\SysOW64
Opens: C:\Windows\SysOW64\sechost.dll
Opens:
C:\windows\temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.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\SysOW64\msimg32.dll
Opens: C:\windows\temp\VERSION.dll
Opens: C:\Windows\SysOW64\version.dll
Opens: C:\Windows\SysOW64\imm32.dll
Opens: C:\Windows\WindowsShell.Manifest
Opens: C:\program files\qqd1eae\log.dat
Opens: C:\Windows\SysOW64\ntdll.dll
Opens: C:\windows\temp\msdialg100_D.dll
Opens: C:\Windows\SysOW64\msdialg100_D.dll
Opens: C:\Windows\system\msdialg100_D.dll
Opens: C:\Windows\msdialg100_D.dll
Opens: C:\Windows\SysOW64\Wbem\msdialg100_D.dll
Opens: C:\Windows\SysOW64\WindowsPowerShell\v1.0\msdialg100_D.dll
Opens: C:\windows\temp\MFC90ENut.dll
Opens: C:\Windows\SysOW64\MFC90ENut.dll
Opens: C:\Windows\system\MFC90ENut.dll
Opens: C:\Windows\MFC90ENut.dll
Opens: C:\Windows\SysOW64\Wbem\MFC90ENut.dll
Opens: C:\Windows\SysOW64\WindowsPowerShell\v1.0\MFC90ENut.dll
Opens: C:\windows\temp\Afx100net.dll
Opens: C:\Windows\SysOW64\Afx100net.dll
Opens: C:\Windows\system\Afx100net.dll
Opens: C:\Windows\Afx100net.dll
Opens: C:\Windows\SysOW64\Wbem\Afx100net.dll
Opens: C:\Windows\SysOW64\WindowsPowerShell\v1.0\Afx100net.dll
Opens: C:\program files\qqd1eae\Log.dat
Opens: C:\Program Files\QQd1eae\slowt64.dll
Opens: C:\Windows\SysOW64\rpcss.dll
Opens: C:\Windows\SysOW64\uxtheme.dll
Opens: C:\Users\Admin\AppData\Local\Temp\restart.dat
Opens: C:\windows\temp\dwmmapi.dll
Opens: C:\Windows\SysOW64\dwmmapi.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\SysOW64\en-US\user32.dll.mui
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\SysOW64\uxtheme.dll.Config
Opens: C:\Windows\SysOW64\ieframe.dll
Opens: C:\Windows\SysOW64\oleacc.dll
Opens: C:\windows\temp\OLEACCRC.DLL
Opens: C:\Windows\SysOW64\oleaccrc.dll
Opens:
C:\Windows\Temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
Opens: C:\Windows\SysOW64\ole32.dll
Opens: C:\windows\temp\ntmarta.dll
Opens: C:\Windows\SysOW64\ntmarta.dll
Opens: C:\Windows\SysOW64\en-US\urlmon.dll.mui
Opens: C:\Windows\SysOW64\shell32.dll
Opens: C:\windows\temp\apphelp.dll
Opens: C:\Windows\SysOW64\apphelp.dll
Opens: C:\WINDOWS\Temp\MJPGC.TMP
Opens: C:\Windows\SysOW64\en-US\ieframe.dll.mui
Opens: C:\Windows\SysOW64\wininet.dll
Opens: C:\windows\temp\profapi.dll
Opens: C:\Windows\SysOW64\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\SysOW64\dnsapi.dll
Opens: C:\windows\temp\iphlpapi.DLL

```

Opens: C:\Windows\SysOW64\IPHLPAPI.DLL
Opens: C:\Windows\temp\WINNSI.DLL
Opens: C:\Windows\SysOW64\winnsi.dll
Opens: C:\Windows\temp\RASAPI32.dll
Opens: C:\Windows\SysOW64\rasapi32.dll
Opens: C:\Windows\temp\rasman.dll
Opens: C:\Windows\SysOW64\rasman.dll
Opens: C:\Windows\temp\rtutils.dll
Opens: C:\Windows\SysOW64\rtutils.dll
Opens: C:\ProgramData\Microsoft\Network\Connections\Pbk\
Opens: C:\Windows\SysOW64\ras
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk
Opens: C:\Windows\temp\sensapi.dll
Opens: C:\Windows\SysOW64\SensApi.dll
Opens: C:\Windows\SysOW64\nlaapi.dll
Opens: C:\Windows\temp\rasadhlp.dll
Opens: C:\Windows\SysOW64\rasadhlp.dll
Opens: C:\Windows\SysOW64\mswsock.dll
Opens: C:\Windows\SysOW64\WSHtcpip.DLL
Opens: C:\Windows\temp\MLANG.dll
Opens: C:\Windows\SysOW64\mlang.dll
Opens: C:\Windows\SysOW64\wship6.dll
Opens: C:\Windows\temp\dhcpcsvc6.DLL
Opens: C:\Windows\SysOW64\dhcpcsvc6.dll
Opens: C:\Program Files (x86)\Common Files\microsoft shared\ink\tipsf.dll
Opens: C:\Windows\temp\dhcpcsvc.DLL
Opens: C:\Windows\SysOW64\dhcpcsvc.dll
Opens: C:\Windows\System32\drivers\etc\hosts
Opens: C:\Windows\SysOW64\FWPuclnt.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\SysOW64\mshtml.dll
Opens: C:\Windows\SysOW64\msls31.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\index[1].php
Opens: C:\Windows\SysOW64\msimtf.dll
Opens: C:\Windows\SysOW64\jscript.dll
Opens: C:\Windows\temp\CRYPTSP.dll
Opens: C:\Windows\SysOW64\cryptsp.dll
Opens: C:\Windows\SysOW64\rsaenh.dll
Opens: C:\Windows\temp\RpcRtRemote.dll
Opens: C:\Windows\SysOW64\RpcRtRemote.dll
Opens: C:\Windows\SysOW64\iepeers.dll
Opens: C:\Windows\SysOW64\winspool.drv
Opens: C:\Windows\SysOW64\dxtrans.dll
Opens: C:\Windows\SysOW64\atl.dll
Opens: C:\Windows\SysOW64\ddrawex.dll
Opens: C:\Windows\SysOW64\ddraw.dll
Opens: C:\Windows\SysOW64\dciman32.dll
Opens: C:\Windows\SysOW64\en-US\setupapi.dll.mui
Opens: C:\Windows\win.ini
Opens: C:\Windows\SysOW64\en-US\ddraw.dll.mui
Opens: C:\Windows\SysOW64\dxtransft.dll
Opens: C:\Windows\temp\ImgUtil.dll
Opens: C:\Windows\SysOW64\imgutil.dll
Opens: C:\Windows\SysOW64\pngfilt.dll
Opens: C:\Windows\temp\SXS.DLL
Opens: C:\Windows\SysOW64\sxs.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\jquery-1.10.2.min_f2fb5194[1].js
Opens: C:\Windows\SysOW64\kernel32.dll
Opens: C:\Windows\Fonts\arial.ttf
Opens: C:\Windows\SysOW64\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\SysOW64\tzres.dll
Opens: C:\Windows\SysOW64\en-US\tzres.dll.mui
Opens: C:\Windows\SysOW64\en-US\jscript.dll.mui
Opens: C:\Windows\SysOW64\en-US\KernelBase.dll.mui
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\SysOW64\d3dim700.dll
Opens: C:\Windows\SysOW64\en-US\mshtml.dll.mui
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\all_async_search_d0d1b2ec[1].js
Opens: C:\Windows\SysOW64\stdole2.tlb
Opens: C:\Windows\SysOW64\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:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\TZILKL9J\every_cookie_aa168cb4[1].js
Opens: C:\Windows\SysWOW64\urlmon.dll
Opens: C:\
Opens: C:\Windows\SysWOW64\Macromed\Flash\Flash10h.ocx
Opens: C:\Windows\SysWOW64\Macromed\Flash\WINMM.dll
Opens: C:\Windows\SysWOW64\winmm.dll
Opens: C:\Windows\SysWOW64\Macromed\Flash\DSOUND.dll
Opens: C:\Windows\SysWOW64\dsound.dll
Opens: C:\Windows\SysWOW64\Macromed\Flash\POWRPROF.dll
Opens: C:\Windows\SysWOW64\powrprof.dll
Opens: C:\Windows\SysWOW64\Macromed\Flash\mcsms.dll
Opens: C:\Windows\SysWOW64\mcsms.dll
Opens: C:\Windows\SysWOW64\Macromed\Flash\USERENV.dll
Opens: C:\Windows\SysWOW64\userenv.dll
Opens: C:\Windows\SysWOW64\Macromed\Flash\ss.sgn
Opens: C:\Windows\SysWOW64\Macromed\Flash
Opens: C:\Windows\SysWOW64\Macromed\Flash\ss.cfg
Opens: C:\Windows\SysWOW64\Macromed\Flash\mms.cfg
Opens: C:\Windows\SysWOW64\Macromed\Flash\oem.cfg
Opens: C:\Windows\SysWOW64\oem.cfg
Opens: C:\Users\Admin\AppData\Roaming\Adobe\Flash Player\AssetCache
Opens: C:\Users\Admin\AppData\Roaming\Adobe\Flash Player\
Opens: C:\Users\Admin\AppData\Roaming\Adobe\Flash Player
Opens: C:\Users\Admin\AppData\Roaming\Adobe
Opens: C:\Users\Admin\AppData\Roaming\Adobe\Flash Player\AssetCache\QW4AL2EV
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\MW60WM90\nu_instant_search_ebeb5baa[1].js
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\VU73CBGV\www.baidu[1].xml
Opens: C:\Windows\temp\XmlLite.dll
Opens: C:\Windows\SysWOW64\xmlite.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\bdsug_async_1cb857eb[1].js
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\env_beb83b45[1].swf
Opens: C:\Windows\temp\MMDevAPI.DLL
Opens: C:\Windows\SysWOW64\MMDevAPI.dll
Opens: C:\Windows\temp\PROPSYS.dll
Opens: C:\Windows\SysWOW64\propsys.dll
Opens: C:\Windows\SysWOW64\msxml3.dll
Opens: C:\Windows\SysWOW64\msxml3r.dll
Opens: C:\Windows\SysWOW64\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\JEQSE8W1
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\2I2VAGUP
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\MW2QSI24
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\UIMZBC64
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData*.2I2VAGUP\desktop.ini
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\JEQSE8W1\desktop.ini
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\MW2QSI24\desktop.ini
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\UIMZBC64\desktop.ini
Opens: C:\Windows\temp\Secur32.dll
Opens: C:\Windows\SysWOW64\secur32.dll
Opens: C:\Windows\temp\credssp.dll
Opens: C:\Windows\SysWOW64\credssp.dll
Opens: C:\Windows\SysWOW64\schannel.dll
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
Opens: C:\Users\Admin\AppData\Roaming\Macromedia\
Opens: C:\Users\Admin\AppData\Roaming\Macromedia
Opens: C:\Users\Admin\AppData
Opens: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HHYYWDWK
Opens: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HHYYWDWK\macromedia.com\support\flashplayer\sys\settings.sol
Opens: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HHYYWDWK\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\macromedia.com\support\flashplayer\sys\
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
Opens: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\
Opens: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support
Opens: C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\macromedia.com\
Opens: C:\Users\Admin\AppData\Roaming\Macromedia\Flash Player\macromedia.com
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\HHYYWDWK\s1.bdstatic.com\sharedObjectBIDUPSID.sol

Opens: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HHYYWDWK\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\HHYYWDWK\macromedia.com\support\flashplayer\sys\s1.bdstatic.com\settings.sol
Opens: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HHYYWDWK\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\s1.bdstatic.com
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\#SharedObjects\HHYYWDWK\s1.bdstatic.com
Opens: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HHYYWDWK\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\JEqSE8W1\userDataBIDUPSID[1].xml
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.ver0x0000000000000001.db
Opens: C:\Users\desktop.ini
Opens: C:\Program Files (x86)\Internet Explorer\ieproxy.dll
Opens: C:\Users
Opens: C:\Users\Admin\AppData\Local\Microsoft
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows
Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016040820160409\
Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016040820160409
Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016040820160409\index.dat
Opens: C:\Windows\SysWOW64\en-US\shell32.dll.mui
Opens: C:\Users\Admin\Favorites
Opens: C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico
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\266VNL55\favicon[1].ico
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\baiduia_b45d552b[1].js
Opens: C:\Windows\SysWOW64\en-US\winmm.dll.mui
Opens: C:\Windows\Media\Windows Navigation Start.wav
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\ps_default[1].gif
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\Socket_9a52fc3e[1].swf
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\s[1].txt
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\icons_0e814c16[1].png
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\union[1].gif
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\ps_default[1].gif
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache\index.dat
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\union[1].gif
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\wb[1].gif
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\wb[1].gif
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\wb[1].gif
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\wb[2].gif
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\o_0108[1].swf
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\wb[2].gif
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\wb[2].gif
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\wb[3].gif
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\wb[1].gif
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\wb[3].gif
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\wb[3].gif
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\wb[4].gif
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\wb[2].gif
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\wb[4].gif
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\wb[4].gif
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\wb[5].gif
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\wb[3].gif
Opens: C:\Program Files (x86)\Common Files\Adobe\Acrobat\ActiveX\AcroPDF.dll
Opens:
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc
Opens:

C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvc80.dll
Opens:
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvc80.dll
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\2I2VAGUP\oXMLStore[1].xml
Opens: C:\Program Files (x86)\Java\jre7\bin\deploy.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\wb[5].gif
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\wb[6].gif
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\wb[4].gif
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\wb[6].gif
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\TZILKL9J\index[1].php
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\bd_logo1[1].png
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\jquery-1.10.2.min_f2fb5194[1].js
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\baidu_jgylogo3[1].gif
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\nuomi_510f7472[1].png
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\zbios_62c636fe[1].png
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\icons_0e814c16[1].png
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\all_async_search_d0d1b2ec[1].js
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\TZILKL9J\every_cookie_aa168cb4[1].js
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\quickdelete_9c14b01a[1].png
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\nu_instant_search_ebeb5baa[1].js
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Internet
Explorer\DOMStore\WU73CBGV\www.baidu[1].xml
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\bd sug_async_1cb857eb[1].js
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\env_beb83b45[1].swf
Writes to: C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\index.dat
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\macromedia.com\support\flashplayer\sys\s1.bdstatic.com\settings.sxx
Writes to: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HHYYWDWK\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
Writes to: C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\JEQSE8W1\UserDataBIDUPSID[1].xml
Writes to:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016040820160409\index.dat
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\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\WM60WM90\baiduia_b45d552b[1].js
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\pc[1].gif
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\ps_default[1].gif
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\ps_default[1].gif
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\ps_default[1].gif
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\ps_default[1].gif
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\ps_default[2].gif
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\JSocket_9a52fc3e[1].swf
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\s[1].txt
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\ps_default[2].gif
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\pc[1].gif
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\u=658147196,2876094505&fm=96&s=418421F0022805031201C81C030050DB[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\u=2752145054,3166876123&fm=58[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL55\u=2521629668,33371966&fm=96&s=6692772A5E7DF07E68DE8D70100COA3[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\u=4267309876,3923431364&fm=96&s=EA90E90821C392A6BCAFF10D0300E0E1[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\u=2719784904,580575759&fm=58[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\u=2731110358,2228192387&fm=58[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\u=2627075135,3105681134&fm=58[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\TZILKL9J\u=2269530877,797123279&fm=96&s=FB1A4A81CFB4358A302555930300B092[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\u=2413434242,1825510918&fm=96&s=4E9241887E120FDE0C4DF0800300E081[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\u=918841094,1711827117&fm=58[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\u=2584046138,590027024&fm=96&s=4E9274884A700F8ACA30D956030050E0[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\his[1]
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\u=1010662780,933723174&fm=58[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\u=3841058258,2231097427&fm=58[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\u=2916809114,3153528632&fm=96&s=1EF66984415003CA44803596030080C2[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\u=4121919617,900972282&fm=58[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\u=2781679007,565939595&fm=58[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\ielib_0108[1].js
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\u=532204567,887570784&fm=58[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\u=2177447570,2292449148&fm=82&s=21904D3064EAEF090584C9C6010070A3&w=121&h=81&img[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\u=1489011112,1613214565&fm=58[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\u=1779799337,1886987922&fm=58[1].jpg
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\o_0108[1].swf
Writes to: C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\2I2VAGUP\oXMLStore[1].xml
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\ps_fp[1].htm
Reads from: C:\Windows\Fonts\StaticCache.dat
Reads from:
C:\Windows\Temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
Reads from: C:\Windows\System32\drivers\etc\hosts
Reads from: C:\Windows\win.ini
Reads from: C:\Windows\SysWow64\dxtmsft.dll
Reads from: C:\Windows\SysWow64\dxtrans.dll
Reads from: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\jquery-1.10.2.min_f2fb5194[1].js
Reads from: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\all_async_search_d0d1b2ec[1].js
Reads from: C:\Windows\SysWow64\iepeers.dll
Reads from: C:\Windows\SysWow64\stdole2.tlb
Reads from: C:\Windows\SysWow64\mshtml.tlb
Reads from: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\every_cookie_aa168cb4[1].js
Reads from: C:\Windows\SysWow64\Macromed\Flash\mms.cfg
Reads from: C:\Windows\SysWow64\Macromed\Flash\Flash10h.ocx
Reads from: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\nu_instant_search_ebeb5baa[1].js
Reads from: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\env_beb83b45[1].swf
Reads from: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\#SharedObjects\HHYYWDWK\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
Reads from: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\bdsug_async_1cb857eb[1].js
Reads from: C:\Windows\SysWow64\ieframe.dll
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\266VNL5S\favicon[1].ico
Reads from: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\baiduia_b45d552b[1].js
Reads from: C:\Users\Admin\AppData\Roaming\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sxx
Reads from: C:\Windows\Media\Windows Navigation Start.wav
Reads from: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\JSocket_9a52fc3e[1].swf
Reads from: C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\JEQSE8W1\UserDataBIDUPSID[1].xml
Reads from: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\icons_0e814c16[1].png
Reads from: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\o_0108[1].swf
Reads from: C:\Users\Admin\AppData\Roaming\Microsoft\Internet
Explorer\UserData\2I2VAGUP\oXMLStore[1].xml
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\settings.sxx
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\#SharedObjects\HHYYWDWK\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
Deletes:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.baidu[2].txt

Network Events

DNS query:	www.baidu.com
DNS query:	s1.bdstatic.com
DNS query:	fpdownload2.macromedia.com
DNS query:	b1.bdstatic.com

DNS query:	ecmb.bding.com
DNS query:	i7.baidu.com
DNS query:	i8.baidu.com
DNS query:	i9.baidu.com
DNS query:	t10.baidu.com
DNS query:	t12.baidu.com
DNS query:	t11.baidu.com
DNS query:	sclick.baidu.com
DNS query:	suggestion.baidu.com
DNS query:	c.baidu.com
DNS query:	sestat.baidu.com
DNS query:	eclick.baidu.com
DNS response:	www.a.shifen.com ⇒ 14.215.177.37
DNS response:	www.a.shifen.com ⇒ 14.215.177.38
DNS response:	wwwbaidu.jomodns.com ⇒ 119.146.74.40
DNS response:	a1293.d.akamai.net ⇒ 58.27.86.10
DNS response:	a1293.d.akamai.net ⇒ 58.27.86.66
DNS response:	bcs.jomodns.com ⇒ 180.97.66.39
DNS response:	t1.n.shifen.com ⇒ 180.97.33.30
DNS response:	image.jomodns.com ⇒ 119.146.74.49
DNS response:	base64.jomodns.com ⇒ 119.146.74.49
DNS response:	suggestion.a.shifen.com ⇒ 14.215.177.44
DNS response:	s.a.shifen.com ⇒ 123.125.115.95
DNS response:	c.e.shifen.com ⇒ 123.125.114.64
DNS response:	sestat.a.shifen.com ⇒ 183.232.231.92
DNS response:	eclick.e.shifen.com ⇒ 123.125.115.164
Connects to:	8.8.8.8:53
Connects to:	14.215.177.37:80
Connects to:	127.0.0.1:63962
Connects to:	119.146.74.40:80
Connects to:	58.27.86.10:80
Connects to:	180.97.66.39:80
Connects to:	180.97.33.30:80
Connects to:	119.146.74.49:80
Connects to:	14.215.177.44:80
Connects to:	123.125.115.95:80
Connects to:	123.125.114.64:80
Connects to:	183.232.231.92:80
Connects to:	123.125.115.164:80
Sends data to:	8.8.8.8:53
Sends data to:	127.0.0.1:63962
Sends data to:	www.a.shifen.com:80 (14.215.177.37)
Sends data to:	wwwbaidu.jomodns.com:80 (119.146.74.40)
Sends data to:	a1293.d.akamai.net:80 (58.27.86.10)
Sends data to:	bcs.jomodns.com:80 (180.97.66.39)
Sends data to:	base64.jomodns.com:80 (119.146.74.49)
Sends data to:	t1.n.shifen.com:80 (180.97.33.30)
Sends data to:	suggestion.a.shifen.com:80 (14.215.177.44)
Sends data to:	s.a.shifen.com:80 (123.125.115.95)
Sends data to:	c.e.shifen.com:80 (123.125.114.64)
Sends data to:	sestat.a.shifen.com:80 (183.232.231.92)
Sends data to:	eclick.e.shifen.com:80 (123.125.115.164)
Receives data from:	8.8.8.8:53
Receives data from:	127.0.0.1:63962
Receives data from:	www.a.shifen.com:80 (14.215.177.37)
Receives data from:	wwwbaidu.jomodns.com:80 (119.146.74.40)
Receives data from:	a1293.d.akamai.net:80 (58.27.86.10)
Receives data from:	bcs.jomodns.com:80 (180.97.66.39)
Receives data from:	t1.n.shifen.com:80 (180.97.33.30)
Receives data from:	base64.jomodns.com:80 (119.146.74.49)
Receives data from:	s.a.shifen.com:80 (123.125.115.95)
Receives data from:	c.e.shifen.com:80 (123.125.114.64)
Receives data from:	sestat.a.shifen.com:80 (183.232.231.92)
Receives data from:	eclick.e.shifen.com:80 (123.125.115.164)

Windows Registry Events

Creates key:	HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_scripturl_mitigation	
Creates key:	HKCU\software\explore
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings
Creates key:	HKLM\software\wow6432node\microsoft\tracing
Creates key:	HKLM\software\wow6432node\microsoft\tracing\rasapi32
Creates key:	HKLM\software\wow6432node\microsoft\tracing\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\p3p\history	
Creates key:	HKLM\software\wow6432node\microsoft\directdraw\mostrecentapplication
Creates key:	HKCU\software\microsoft\windows script\settings
Creates key:	HKLM\software\wow6432node\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\mshist012016040820160409	
Creates key:	HKCU\software\microsoft\internet explorer\main\windowssearch
Creates key:	HKLM\software\wow6432node\microsoft\downloadmanager
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[proxybypass]	
Deletes value:	HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap[proxybypass]	
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap[intranetname]
Deletes value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap[intranetname]
Deletes value: HKCU\software\microsoft\windows\currentversion\internet
settings\proxyserver]
Deletes value: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
Deletes value: HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
Deletes value: HKCU\software\macromedia\flashplayer[flashplayerversion]
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\software\wow64
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\language
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings
Opens key: HKLM\software\policies\microsoft\mui\settings
Opens key: HKCU\
Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop\languageconfiguration
Opens key: HKCU\control panel\desktop
Opens key: HKCU\control panel\desktop\muicached
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key: HKLM\
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\diagnostics
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\wow6432node\microsoft\ole
Opens key: HKLM\software\wow6432node\microsoft\ole\tracing
Opens key: HKLM\software\microsoft\ole\tracing
Opens key: HKLM\software\wow6432node\microsoft\oleaut
Opens key: HKLM\system\currentcontrolset\services\crypt32
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings
Opens key: HKCU\software\microsoft\internet explorer\main
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol
Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
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\wow6432node\microsoft\windows
nt\currentversion\fontsubstitutes
Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
Opens key:
HKLM\software\wow6432node\microsoft\ctf\compatibility\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.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\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}
Opens key: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
Opens key: HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\treatas
Opens key: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\progid
Opens key: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler

Opens key: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler

Opens key: HKLM\software\wow6432node\microsoft\rpc

Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername

Opens key: HKLM\system\setup

Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc

Opens key: HKLM\software\policies\microsoft\windows nt\rpc

Opens key: HKLM\software\policies\microsoft\sqlclient\windows

Opens key: HKLM\software\microsoft\sqlclient\windows

Opens key: HKCU\software\classes\wow6432node\clsid\{889d2feb-5411-4565-8998-1dd2c5261283}

Opens key: HKCR\wow6432node\clsid\{889d2feb-5411-4565-8998-1dd2c5261283}

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\wow6432node\policies\microsoft\windows\app management

Opens key: HKLM\software\policies\microsoft\windows\app management

Opens key: HKCU\software\classes\wow6432node\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}

Opens key: HKCR\wow6432node\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}

Opens key: HKCU\software\classes\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}

Opens key: HKCR\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}

Opens key: HKLM\software\wow6432node\microsoft\ctf\tip\{000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}

Opens key: HKLM\software\microsoft\ctf\tip\{000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}

Opens key: HKLM\software\wow6432node\microsoft\ctf\

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

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

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

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

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

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562

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

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

Opens key: HKLM\system\currentcontrolset\control\lsa\accessproviders

Opens key: HKLM\system\currentcontrolset\services\ldap

Opens key: HKCU\software\microsoft\internet explorer\ietld

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

Opens key: HKLM\software\wow6432node\policies\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\wow6432node\microsoft\windows\currentversion\policies\explorer

Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer

Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\62ddfbbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe

Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder

Opens key: HKCR\wow6432node\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\wow6432node\microsoft\windows\currentversion\policies\nonenum

Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32

Opens key: HKLM\software\wow6432node\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\wow6432node\policies\microsoft\windows\appcompat

Opens key: HKLM\software\policies\microsoft\windows\appcompat

Opens key: HKCU\software\microsoft\windows\currentversion\shell extensions\cached

Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}

Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}

Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas

Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas

Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\progid

Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\progid

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}\progid

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\progid

Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler

Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler

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

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

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

Opens key: HKCU\software\policies\microsoft\internet explorer\browseremulation

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

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\accepted documents

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\ratings

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\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615

Opens key: HKLM\software\wow6432node\policies

Opens key: HKCU\software\policies

Opens key: HKCU\software

Opens key: HKLM\software\wow6432node

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

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915

Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\

Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains

Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\

Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\

Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges

Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\

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

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

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

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001

Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap

Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap

Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap

Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\ranges\

Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\protocoldefaults\

Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\domains\

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zonemap\domains\

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

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\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\

Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones

Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\

Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\0

Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\0

Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\0

Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\1

Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\1

Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\1

Opens key:	HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap\	
Opens key:	HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\2
Opens key:	HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2	
Opens key:	HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2	
Opens key:	HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\3
Opens key:	HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3	
Opens key:	HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3	
Opens key:	HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\4
Opens key:	HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4	
Opens key:	HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4	
Opens key:	HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown	
Opens key:	HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown	
Opens key:	HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\	
Opens key:	HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones	
Opens key:	HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\	
Opens key:	HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\	
Opens key:	HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0	
Opens key:	HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0	
Opens key:	HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0	
Opens key:	HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0	
Opens key:	HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1	
Opens key:	HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1	
Opens key:	HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1	
Opens key:	HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1	
Opens key:	HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2	
Opens key:	HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2	
Opens key:	HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2	
Opens key:	HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2	
Opens key:	HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3	
Opens key:	HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3	
Opens key:	HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3	
Opens key:	HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3	
Opens key:	HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4	
Opens key:	HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache	
Opens key:	HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache	
Opens key:	HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content	
Opens key:	HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\content	
Opens key:	HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
Opens key:	HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}
Opens key:	HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}\propertybag
Opens key:	HKCU\software\microsoft\windows\currentversion\explorer
Opens key:	HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
Opens key:	HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
Opens key:	HKCU\software\microsoft\windows\currentversion\explorer\user shell
Opens key:	HKLM\software\wow6432node\policies\microsoft\windows\explorer
Opens key:	HKLM\software\policies\microsoft\windows\explorer

Opens key: HKCU\software\policies\microsoft\windows\explorer
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4cf-9d55-7b8e7f157091}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4cf-9d55-7b8e7f157091}\propertybag
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}\propertybag
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}\propertybag
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\history
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\5.0\cache
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
Opens key: HKLM\software\wow6432node\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\wow6432node\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\381e2851
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
Opens key: HKLM\software\wow6432node\microsoft\tracing\rasapi32
Opens key: HKLM\software\wow6432node\microsoft\tracing\rasmancs
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist
Opens key: HKLM\software\microsoft\sqlclient\windows\disabledprocesses\
Opens key: HKLM\software\microsoft\sqlclient\windows\disabledsessions\
Opens key: HKU\
Opens key: HKLM\system\currentcontrolset\control\sqlservicelist
Opens key: HKLM\system\currentcontrolset\services\dnsclient\parameters
Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient
Opens key: HKLM\system\currentcontrolset\services\dns
Opens key: HKLM\software\wow6432node\policies\microsoft\windows
nt\dnsclient\dnsconfig
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient\dnsconfig
Opens key: HKLM\system\currentcontrolset\services\dnsclient\parameters\dnsconfig
Opens key: HKCU\software\microsoft\internet explorer
Opens key: HKLM\software\wow6432node\microsoft\internet explorer
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_mime_handling
Opens key: HKCU\software\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*\br/>Opens key: HKCR\protocols\name-space handler*\br/>Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_compat_logging
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_enable_compat_logging
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\user
agent
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\user agent
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\user agent
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\user agent
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\user agent
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\user agent\ua tokens
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\user agent\pre platform
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\user agent\pre platform
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\pre platform
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\user agent\post platform
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\user agent\post platform
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\post platform
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers
Opens key: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
Opens key: HKCU\software\microsoft\windows\currentversion\urlmon settings
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
Opens key: HKCU\software\microsoft\internet explorer\international
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_legacy_compression
Opens key: HKLM\software\wow6432node\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\wow6432node\microsoft\windows\currentversion\explorer\travellog
Opens key: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
Opens key: HKLM\software\wow6432node\policies\microsoft\system\dnsclient
Opens key: HKLM\software\policies\microsoft\system\dnsclient
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\wow6432node\microsoft\windows\currentversion\explorer\autocomplete
Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}
Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}
Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\treatas
Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\progid
Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\progid
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}\progid
Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandler
Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandler
Opens key: HKLM\system\currentcontrolset\services\dns\parameters\dns\cache
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}
Opens key: HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}
Opens key: HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}
Opens key: HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\treatas
Opens key: HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\progid
Opens key: HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\progid
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}\progid
Opens key: HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprochandler
Opens key: HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprochandler
Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}
Opens key: HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}
Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\treatas
Opens key: HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\progid
Opens key: HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\progid
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}\progid
Opens key: HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprochandler
Opens key: HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprochandler
Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}
Opens key: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}
Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treatas
Opens key: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\progid
Opens key: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\progid
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}\progid
Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandler
Opens key: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandler
Opens key: HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete\client\
Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}
Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}
Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treatas
Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\progid
Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}

b61bb7cdd997}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprochandler
Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprochandler
Opens key: HKLM\software\wow6432node\microsoft\rpc\extensions
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\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e963}
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e963}
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a91d0a5e-390e-4979-9c38-127795cce47a}
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b9ec5865-2d36-4cb8-b474-65fee5bae0b1}
Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage
Opens key: HKCU\software\microsoft\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\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_feeds
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_feeds
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject
Opens key: HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}
Opens key: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
Opens key: HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\treatas
Opens key: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\progid
Opens key: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprochandler
Opens key: HKCR\wow6432node\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\wow6432node\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\wow6432node\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\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_aria_support
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams
Opens key: HKLM\software\wow6432node\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\wow6432node\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\wow6432node\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\wow6432node\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\wow6432node\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\wow6432node\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\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr
Opens key: HKLM\software\wow6432node\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\wow6432node\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\wow6432node\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\wow6432node\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\wow6432node\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\wow6432node\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_fl
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fl
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\app
paths\outlook.exe
Opens key: HKLM\software\microsoft\windows\currentversion\app_paths\outlook.exe
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\application
compatibility
Opens key: HKLM\software\wow6432node\policies\microsoft\internet
explorer\domstorage
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\wow6432node\microsoft\internet explorer\domstorage
Opens key: HKLM\software\wow6432node\policies\microsoft\internet
explorer\safety\privacie
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\wow6432node\microsoft\internet explorer\safety\privacie
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_manage_script_circular_refs
Opens key: HKLM\software\wow6432node\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\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\security\floppy
access
Opens key: HKCU\software\microsoft\internet explorer\security\adv addrbar spoof
detection
Opens key: HKLM\software\wow6432node\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\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}
Opens key: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\treatas
Opens key: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\progid
Opens key: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\progid
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}\progid
Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler
Opens key: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\inprochandler
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_document_compatible_mode
Opens key: HKLM\software\wow6432node\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\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\zoom
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\wow6432node\microsoft\internet explorer\zoom
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_weboc_document_zoom
Opens key: HKLM\software\wow6432node\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\wow6432node\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\wow6432node\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\wow6432node\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\wow6432node\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\ntp\codepage
Opens key: HKCU\software\microsoft\internet explorer\international\scripts\3
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\version vector
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones
Opens key: HKLM\software\policies\microsoft\internet explorer\low rights
Opens key: HKCU\software\microsoft\internet explorer\low rights
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\low rights
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\0
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_read_zone_strings_from_registry
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_read_zone_strings_from_registry
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\1
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\2
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\3
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\4
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe
Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\dxtrans
Opens key: HKLM\software\policies\microsoft\internet explorer\dxtrans
Opens key: HKCU\software\microsoft\internet explorer\dxtrans
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\dxtrans
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_sslux
Opens key: HKLM\software\wow6432node\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: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\
Opens key: HKLM\software\wow6432node\policies\microsoft\internet
explorer\restrictions
Opens key: HKLM\software\policies\microsoft\internet explorer\restrictions
Opens key: HKCU\software\policies\microsoft\internet explorer\restrictions
Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}

Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}
Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}\treatas
f4ceaf59cfc}\treatas
Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}\progid
f4ceaf59cfc}\progid
Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}\progid
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}
Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}\progid
f4ceaf59cfc}\progid
Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}\inprocserver32
f4ceaf59cfc}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}\inprocserver32
f4ceaf59cfc}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}\inprochandler32
f4ceaf59cfc}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}\inprochandler32
f4ceaf59cfc}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}\inprochandler
f4ceaf59cfc}\inprochandler
Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}\inprochandler
f4ceaf59cfc}\inprochandler
Opens key: HKCU\software\policies\microsoft\internet explorer\control panel
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_iedde_register_urlecho
explorer\main\featurecontrol\feature_iedde_register_urlecho
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_iedde_register_urlecho
explorer\main\featurecontrol\feature_iedde_register_urlecho
Opens key: HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}
00aa00bbb58}\treatas
Opens key: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}\progid
00aa00bbb58}\progid
Opens key: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}\inprocserver32
00aa00bbb58}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}\inprochandler32
00aa00bbb58}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}\inprochandler32
00aa00bbb58}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}\inprochandler
00aa00bbb58}\inprochandler
Opens key: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}\inprochandler
00aa00bbb58}\inprochandler
Opens key: HKLM\software\wow6432node\microsoft\windows script\features
Opens key: HKLM\software\wow6432node\microsoft\com3
Opens key: HKCU\software\classes\appid\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
Opens key: HKCR\appid\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
Opens key: HKLM\software\wow6432node\microsoft\ole\appcompat
Opens key: HKLM\software\microsoft\ole\appcompat
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider
Opens key: HKLM\system\currentcontrolset\control\lsa\ipsalgorithmpolicy
Opens key: HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
Opens key: HKLM\software\policies\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography
Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload
Opens key: HKCU\software\classes\wow6432node\interface\{0000134-0000-0000-c000-000000000046}
000000000046}\proxystubclsid32
000000000046}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{0000134-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\wow6432node\interface\{0000134-0000-0000-c000-000000000046}\proxystubclsid32
000000000046}\proxystubclsid32
Opens key: HKLM\system\currentcontrolset\services\bfe
Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\recovery
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
explorer\main\featurecontrol\feature_scripturl_mitigation
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_block_lmz_img
explorer\main\featurecontrol\feature_block_lmz_img
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_block_lmz_img
explorer\main\featurecontrol\feature_block_lmz_img
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_behaviors
explorer\main\featurecontrol\feature_behaviors
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\default behaviors
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}
00aa00bdce0b}\treatas
Opens key: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\progid
00aa00bdce0b}\progid
Opens key: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}

00aa00bdce0b}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler
Opens key: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler
Opens key: HKCU\software\policies\microsoft\internet explorer\persistance
Opens key: HKLM\software\wow6432node\policies\microsoft\internet
explorer\persistance
Opens key: HKLM\software\policies\microsoft\internet explorer\persistance
Opens key: HKCU\software\classes\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}
Opens key: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}
Opens key: HKCU\software\classes\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\treatas
Opens key: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\progid
Opens key: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprochandler
Opens key: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprochandler
Opens key: HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}
Opens key: HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}
Opens key: HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\treatas
Opens key: HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\progid
Opens key: HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\progid
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}\progid
Opens key: HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprochandler
Opens key: HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprochandler
Opens key: HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}
Opens key: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}
Opens key: HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\treatas
Opens key: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\progid
Opens key: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\progid
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}\progid
Opens key: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprochandler
Opens key: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprochandler
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\setup
Opens key: HKLM\software\microsoft\windows\currentversion\setup
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion
Opens key: HKLM\hardware\devicemap\video
Opens key: HKLM\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-
1e1a187c13e9}\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\wow6432node\microsoft\directdraw\compatibility
Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\bug!
Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\demolitionderby2
Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\diablo
Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\mortalkombat3
Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\msgolf98
Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nhlpowerplay
Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nortonsysteminfo
Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue
squadron
Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\savage
Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\scorchedplanet
Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\silentthunder
Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft100
Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft115
Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraftdemo
Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\terraced
Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\thirddimension
Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark
Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark
Opens key: HKLM\software\wow6432node\microsoft\directdraw\gammacalibrator
Opens key: HKLM\software\wow6432node\microsoft\directdraw
Opens key: HKLM\software\wow6432node\microsoft\direct3d
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\msasn1
Opens key: HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}
Opens key: HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}
Opens key: HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\treatas
Opens key: HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\progid
Opens key: HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprochandler
Opens key: HKCR\wow6432node\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\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}
Opens key: HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}
Opens key: HKCU\software\classes\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\treatas
Opens key: HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\progid
Opens key: HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprochandler
Opens key: HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprochandler
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\activex
compatibility
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\activex
compatibility\{e71b4063-3e59-11d2-952a-00c04fa34f05}
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\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}
Opens key: HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}
Opens key: HKCU\software\classes\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\treatas
Opens key: HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\progid
Opens key: HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{30c3b080-30fb-11d0-b724-

00aa006c1a01}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprochandler
Opens key: HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprochandler
Opens key: HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}
Opens key: HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}
Opens key: HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\treatas
Opens key: HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\progid
Opens key: HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprochandler
Opens key: HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprochandler
Opens key: HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}
Opens key: HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}
Opens key: HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\treatas
Opens key: HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\progid
Opens key: HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\progid
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}\progid
Opens key: HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\progid
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\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserver32
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\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprochandler
Opens key: HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprochandler
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\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}
Opens key: HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}
Opens key: HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\treatas
Opens key: HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\progid
Opens key: HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprochandler
Opens key: HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprochandler
Opens key: HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}
Opens key: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}

Opens key: HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\treatas

Opens key: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\treatas

Opens key: HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\progid

Opens key: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\progid

Opens key: HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprochandler

Opens key: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprochandler

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\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561

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\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_disable_behaviors_draw_reentrancy

Opens key: HKCU\software\classes\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}

Opens key: HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}

Opens key: HKCU\software\classes\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\treatas

Opens key: HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\treatas

Opens key: HKCU\software\classes\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\progid

Opens key: HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\progid

Opens key: HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}

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\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprochandler

Opens key: HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprochandler

Opens key: HKCU\software\microsoft\internet explorer\international\scripts\26

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\wow6432node\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\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_block_lmz_script

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

Opens key: HKLM\software\wow6432node\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\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_windowedselectcontrol
Opens key: HKCU\software\microsoft\internet explorer\new windows
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\new windows
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_xmlhttp
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_xmlhttp
Opens key: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsum
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_binary_caller_service_provider
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_binary_caller_service_provider
Opens key: HKCU\software\classes\wow6432node\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{332c4425-26cb-11d0-b483-00c04fd90119}
Opens key: HKCR\wow6432node\interface\{332c4425-26cb-11d0-b483-00c04fd90119}
Opens key: HKCU\software\classes\wow6432node\interface\{332c4425-26cb-11d0-b483-00c04fd90119}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{332c4425-26cb-11d0-b483-00c04fd90119}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}
Opens key: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\treatas
Opens key: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\progid
Opens key: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\progid
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}\progid
Opens key: HKCR\clsid\{00020424-0000-0000-c000-000000000046}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\inprochandler
Opens key: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\inprochandler
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\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\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas
Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid
Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid
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}\progid
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler
Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler
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\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}
Opens key: HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}
Opens key: HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\treatas
Opens key: HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\progid
Opens key: HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprochandler
Opens key: HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprochandler
Opens key: HKLM\hardware\description\system\centralprocessor\0
Opens key: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider
types\type 001
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\microsoft\internet explorer\main\featurecontrol\feature_activex_repurposedetection
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_activex_repurposedetection
Opens key: HKLM\software\wow6432node\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\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_addon_management
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_alloweddomainlist
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_alloweddomainlist
Opens key: HKCU\software\wow6432node\microsoft\internet explorer\extension compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}
Opens key: HKCU\software\classes\wow6432node\clsid\{aaf8c6ce-f972-11d0-97eb-00aa00615333}
Opens key: HKCR\wow6432node\clsid\{aaf8c6ce-f972-11d0-97eb-00aa00615333}
Opens key: HKCU\software\microsoft\code store database\distribution units
Opens key: HKLM\software\wow6432node\microsoft\code store database\distribution units\{d27cdb6e-ae6d-11cf-96b8-444553540000}
Opens key: HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\availableversion
Opens key: HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\availableversion
Opens key: HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\installedversion
Opens key: HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\installedversion
Opens key: HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\appid
Opens key: HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\appid
Opens key: HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\languagecheckperiod
Opens key: HKCR\wow6432node\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\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_consult_mime_killbit_kb905915
Opens key: HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\miscstatus
Opens key: HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\miscstatus
Opens key: HKCU\software\classes\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\1
Opens key: HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\1
Opens key: HKLM\software\wow6432node\microsoft\windows\tablet pc
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_domstorage
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_domstorage
Opens key: HKCU\software\microsoft\internet explorer\feed discovery
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\feed discovery
Opens key: HKCU\software\microsoft\ftp
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: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32
Opens key: HKCU\software\classes\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}
Opens key: HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}
Opens key: HKCU\software\classes\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\treatas
Opens key: HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\progid
Opens key: HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprocserver32
Opens key: HKCU\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
Opens key: HKCU\software\classes\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprochandler
Opens key: HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprochandler
Opens key: HKCU\software\microsoft\windows\currentversion\multimedia\midimap
Opens key: HKLM\software\wow6432node\microsoft\msxml30
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\userdata
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\wow6432node\microsoft\windows\currentversion\policies\system
Opens key: HKLM\software\microsoft\windows\currentversion\policies\system
Opens key: HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
Opens key: HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
Opens key: HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\treatas
Opens key: HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\progid
Opens key: HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\progid
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}\progid
Opens key: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprochandler
Opens key: HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprochandler
Opens key: HKCU\software\classes\wow6432node\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}
Opens key: HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}
Opens key: HKCU\software\classes\wow6432node\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\forward
Opens key: HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\forward
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\wow6432node\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib
Opens key: HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib
Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\services
Opens key: HKLM\software\policies\microsoft\internet explorer\services
Opens key: HKCU\software\microsoft\internet explorer\services
Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\activities
Opens key: HKLM\software\policies\microsoft\internet explorer\activities
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\microsoft\internet explorer\activities
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\activities
Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\infodelivery\restrictions
Opens key: HKLM\software\policies\microsoft\internet explorer\infodelivery\restrictions
Opens key: HKCU\software\policies\microsoft\internet explorer\infodelivery\restrictions
Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\suggested sites
Opens key: HKLM\software\policies\microsoft\internet explorer\suggested sites
Opens key: HKCU\software\microsoft\internet explorer\suggested sites
Opens key: HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder
Opens key: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder
Opens key: HKCU\software\classes\wow6432node\interface\{00020400-0000-0000-c000-000000000046}
Opens key: HKCR\wow6432node\interface\{00020400-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\wow6432node\interface\{00020400-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{00020400-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}
Opens key: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}\treatas
Opens key: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}\progid
Opens key: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}\progid
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}\progid
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\progid
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder
Opens key: HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32
Opens key: HKLM\software\wow6432node\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\{8063a3d4-8213-11e3-a68e-806e6f6e6963}\
Opens key: HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}\inprochandler
Opens key: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}\inprochandler
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\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-11e3-a68e-806e6f6e6963}\
Opens key: HKCU\software\classes\wow6432node\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}
Opens key: HKCR\wow6432node\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}
Opens key: HKCU\software\classes\wow6432node\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
Opens key: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
Opens key: HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid
Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid
Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\progid
Opens key: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\progid
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}\progid
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\progid
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}\progid

Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler
Opens key: HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler32
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\Opens key: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler
Opens key: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler
Opens key: HKLM\software\wow6432node\microsoft\windows\shell\registeredapplications\urlassociations\directory\openwithprogid
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: 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: HKCU\software\classes\wow6432node\interface\{00020404-0000-0000-c000-000000000046}
Opens key: HKCR\wow6432node\interface\{00020404-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\wow6432node\interface\{00020404-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{00020404-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}
Opens key: HKCR\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}\treatas
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\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}\progid
Opens key: HKCR\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}\progid
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}\progid
Opens key: HKCR\clsid\{00020421-0000-0000-c000-000000000046}\progid
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\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}\inprocserver32
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: HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}\inprochandler
Opens key: HKCR\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}\inprochandler
Opens key: HKLM\software\wow6432node\microsoft\windows\shell\registeredapplications\urlassociations\directory\openwithprogid
Opens key: HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
Opens key: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
Opens key: HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}

```
444553540000}\inprocserver32
  Opens key: HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\shellfolder
444553540000}\shellfolder
  Opens key: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\shellfolder
  Opens key: HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\treatas
  Opens key: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\treatas
  Opens key: HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\progid
  Opens key: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\progid
  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}\progid
  Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\progid
  Opens key: HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandler32
  Opens key: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandler32
  Opens key: HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandler
  Opens key: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandler
  Opens key: HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandler
  Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\objects\{ff393560-c2a7-11cf-bff4-444553540000}
  Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016040820160409
  Opens key: HKCU\software\microsoft\windows\currentversion\app paths\62ddbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
  Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\app paths\62ddbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
  Opens key: HKLM\software\microsoft\windows\currentversion\app paths\62ddbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.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\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
  Opens key: HKCR\wow6432node\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\wow6432node\microsoft\internet explorer\feeds
  Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}
  Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}\propertybag
  Opens key: HKLM\software\wow6432node\microsoft\windows search
  Opens key: HKCU\software\classes\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}
  Opens key: HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}
  Opens key: HKCU\software\classes\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\treatas
  Opens key: HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\treatas
  Opens key: HKCU\software\classes\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\progid
  Opens key: HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\progid
  Opens key: HKCU\software\classes\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprocserver32
  Opens key: HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprocserver32
  Opens key: HKCU\software\classes\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprochandler32
  Opens key: HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprochandler32
  Opens key: HKCU\software\classes\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprochandler
  Opens key: HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\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\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_mime_treat_image_as_authoritative
  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\microsoft\internet explorer\main\featurecontrol\feature_isolate_named_windows
  Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_isolate_named_windows
  Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_disable_navigation_sounds
  Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_disable_navigation_sounds
  Opens key: HKCU\appproxy\schemas\apps\explorer\navigating\current
  Opens key: HKCU\appproxy\schemas\
  Opens key: HKCU\appproxy\schemas\apps\explorer\navigating\current\active
  Opens key: HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}
  Opens key: HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}
  Opens key: HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\treatas
```


Opens key: HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\progid
Opens key: HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\progid
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}\progid
Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprochandler
Opens key: HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprochandler
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\microsoft\internet explorer\searchproviders\internet
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_additional_ie8_memory_cleanup
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_additional_ie8_memory_cleanup
Opens key: HKCU\appevents\schemes\apps\explorer\activatingdocument\current
Opens key: HKCU\software\classes\mime\database\content type\image/jpeg
Opens key: HKCR\mime\database\content type\image/jpeg
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\arial
Opens key: HKCU\software\classes\mime\database\content type\baiduapp/json;v6.27.2.14; charset=utf-8
Opens key: HKCR\mime\database\content type\baiduapp/json; v6.27.2.14; charset=utf-8
Opens key: HKCU\software\classes\mime\database\content type\baiduapp/json
Opens key: HKCR\mime\database\content type\baiduapp/json
Opens key: HKCU\software\classes\protocols\filter\baiduapp/json; v6.27.2.14; charset=utf-8
Opens key: HKCR\protocols\filter\baiduapp/json; v6.27.2.14; charset=utf-8
Opens key: HKCU\software\classes\protocols\filter\application/javascript
Opens key: HKCR\protocols\filter\application/javascript
Opens key: HKCU\software\classes\msxml2.xmlhttp
Opens key: HKCR\msxml2.xmlhttp
Opens key: HKCU\software\classes\msxml2.xmlhttp\clsid
Opens key: HKCR\msxml2.xmlhttp\clsid
Opens key: HKCU\software\classes\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}
Opens key: HKCR\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}
Opens key: HKCU\software\classes\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\treatas
Opens key: HKCR\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\progid
Opens key: HKCR\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\inprochandler
Opens key: HKCR\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\inprochandler
Opens key: HKCU\software\classes\shockwaveflash.shockwaveflash.12
Opens key: HKCR\shockwaveflash.shockwaveflash.12
Opens key: HKCU\software\classes\shockwaveflash.shockwaveflash.11
Opens key: HKCR\shockwaveflash.shockwaveflash.11
Opens key: HKCU\software\classes\shockwaveflash.shockwaveflash.10
Opens key: HKCR\shockwaveflash.shockwaveflash.10
Opens key: HKCU\software\classes\shockwaveflash.shockwaveflash.10\clsid
Opens key: HKCR\shockwaveflash.shockwaveflash.10\clsid
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_block_lmz_object
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_block_lmz_object
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\plugins\disableactivexcontrols
Opens key: HKCU\software\classes\swf
Opens key: HKCR\swf
Opens key: HKCU\software\classes\baidubar.tool.1
Opens key: HKCR\baidubar.tool.1
Opens key: HKCU\software\classes\baidubar.tool.2
Opens key: HKCR\baidubar.tool.2
Opens key: HKCU\software\classes\baidubar.tool.3
Opens key: HKCR\baidubar.tool.3
Opens key: HKCU\software\classes\baidubar.tool.4
Opens key: HKCR\baidubar.tool.4
Opens key: HKCU\software\classes\baidubar.tool.5
Opens key: HKCR\baidubar.tool.5
Opens key: HKCU\software\classes\baidubar.tool.6
Opens key: HKCR\baidubar.tool.6
Opens key: HKCU\software\classes\baidubar.tool.7
Opens key: HKCR\baidubar.tool.7
Opens key: HKCU\software\classes\baidubar.tool.8
Opens key: HKCR\baidubar.tool.8
Opens key: HKCU\software\classes\baidubar.tool.9
Opens key: HKCR\baidubar.tool.9

Opens key: HKCU\software\classes\google.oneclickctrl.1
Opens key: HKCR\google.oneclickctrl.1
Opens key: HKCU\software\classes\google.oneclickctrl.2
Opens key: HKCR\google.oneclickctrl.2
Opens key: HKCU\software\classes\google.oneclickctrl.3
Opens key: HKCR\google.oneclickctrl.3
Opens key: HKCU\software\classes\google.oneclickctrl.4
Opens key: HKCR\google.oneclickctrl.4
Opens key: HKCU\software\classes\google.oneclickctrl.5
Opens key: HKCR\google.oneclickctrl.5
Opens key: HKCU\software\classes\google.oneclickctrl.6
Opens key: HKCR\google.oneclickctrl.6
Opens key: HKCU\software\classes\google.oneclickctrl.7
Opens key: HKCR\google.oneclickctrl.7
Opens key: HKCU\software\classes\google.oneclickctrl.8
Opens key: HKCR\google.oneclickctrl.8
Opens key: HKCU\software\classes\google.oneclickctrl.9
Opens key: HKCR\google.oneclickctrl.9
Opens key: HKCU\software\classes\qvodinsert.qvodctrl.1
Opens key: HKCR\qvodinsert.qvodctrl.1
Opens key: HKCU\software\classes\qvodinsert.qvodctrl.2
Opens key: HKCR\qvodinsert.qvodctrl.2
Opens key: HKCU\software\classes\qvodinsert.qvodctrl.3
Opens key: HKCR\qvodinsert.qvodctrl.3
Opens key: HKCU\software\classes\qvodinsert.qvodctrl.4
Opens key: HKCR\qvodinsert.qvodctrl.4
Opens key: HKCU\software\classes\qvodinsert.qvodctrl.5
Opens key: HKCR\qvodinsert.qvodctrl.5
Opens key: HKCU\software\classes\qvodinsert.qvodctrl.6
Opens key: HKCR\qvodinsert.qvodctrl.6
Opens key: HKCU\software\classes\qvodinsert.qvodctrl.7
Opens key: HKCR\qvodinsert.qvodctrl.7
Opens key: HKCU\software\classes\qvodinsert.qvodctrl.8
Opens key: HKCR\qvodinsert.qvodctrl.8
Opens key: HKCU\software\classes\qvodinsert.qvodctrl.9
Opens key: HKCR\qvodinsert.qvodctrl.9
Opens key: HKCU\software\classes\pdf.pdfctrl.2
Opens key: HKCR\pdf.pdfctrl.2
Opens key: HKCU\software\classes\pdf.pdfctrl.3
Opens key: HKCR\pdf.pdfctrl.3
Opens key: HKCU\software\classes\pdf.pdfctrl.4
Opens key: HKCR\pdf.pdfctrl.4
Opens key: HKCU\software\classes\pdf.pdfctrl.5
Opens key: HKCR\pdf.pdfctrl.5
Opens key: HKCU\software\classes\pdf.pdfctrl.6
Opens key: HKCR\pdf.pdfctrl.6
Opens key: HKCU\software\classes\pdf.pdfctrl.7
Opens key: HKCR\pdf.pdfctrl.7
Opens key: HKCU\software\classes\pdf.pdfctrl.8
Opens key: HKCR\pdf.pdfctrl.8
Opens key: HKCU\software\classes\pdf.pdfctrl.9
Opens key: HKCR\pdf.pdfctrl.9
Opens key: HKCU\software\classes\pdf.pdfctrl.1
Opens key: HKCR\pdf.pdfctrl.1
Opens key: HKCU\software\classes\acropdf.pdf.1
Opens key: HKCR\acropdf.pdf.1
Opens key: HKCU\software\classes\acropdf.pdf.1\clsid
Opens key: HKCR\acropdf.pdf.1\clsid
Opens key: HKCU\software\classes\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-444553540000}
Opens key: HKCR\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-444553540000}
Opens key: HKCU\software\classes\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-444553540000}\treatas
Opens key: HKCR\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-444553540000}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-444553540000}\progid
Opens key: HKCR\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-444553540000}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-444553540000}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-444553540000}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-444553540000}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-444553540000}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-444553540000}\inprochandler
Opens key: HKCR\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-444553540000}\inprochandler
Opens key: HKCU\software\adobe\acrobat reader\9.0\originals
Opens key: HKCU\software\adobe\adobe acrobat\9.0\originals
Opens key: HKCU\software\adobe\acrobat reader\8.0\originals
Opens key: HKCU\software\adobe\adobe acrobat\8.0\originals
Opens key: HKCU\software\adobe\acrobat reader\7.0\originals
Opens key: HKCU\software\adobe\adobe acrobat\7.0\originals
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{08b0e5c0-4fcb-11cf-aaa5-00401c608500}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{08b0e5c0-4fcb-11cf-aaa5-00401c608555}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{22d6f312-b0f6-11d0-94ab-0080c74c7e95}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{283807b5-2c60-11d0-a31d-00aa00b92c03}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{3af36230-a269-11d1-b5bf-0000f8051515}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{44bba840-cc51-11cf-aafa-00aa00b6015c}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{44bba842-cc51-11cf-aafa-00aa00b6015b}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed components\{44bba848-cc51-11cf-aafa-00aa00b6015c}
Opens key: HKLM\software\wow6432node\microsoft\active setup\installed

components\{45ea75a0-a269-11d1-b5bf-0000f8051515}
Opens key: HKLM\software\wow6432node\microsoft\active_setup\installed
components\{4f216970-c90c-11d1-b5c7-0000f8051515}
Opens key: HKLM\software\wow6432node\microsoft\active_setup\installed
components\{5a8d6ee0-3e18-11d0-821e-444553540000}
Opens key: HKLM\software\wow6432node\microsoft\active_setup\installed
components\{7790769c-0471-11d2-af11-00c04fa35d02}
Opens key: HKLM\software\wow6432node\microsoft\active_setup\installed
components\{89820200-ecbd-11cf-8b85-00aa005b4340}
Opens key: HKLM\software\wow6432node\microsoft\active_setup\installed
components\{89820200-ecbd-11cf-8b85-00aa005b4383}
Opens key: HKLM\software\wow6432node\microsoft\active_setup\installed
components\{9381d8f2-0288-11d0-9501-00aa00b911a5}
Opens key: HKLM\software\wow6432node\microsoft\active_setup\installed
components\{cc2a9ba0-3bdd-11d0-821e-444553540000}
Opens key: HKLM\software\wow6432node\microsoft\active_setup\installed
components\{de5aed00-a4bf-11d1-9948-00c04f98bbc9}
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
Queries value: HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\system\currentcontrolset\control\locale[empty]
Queries value:
HKLM\system\currentcontrolset\control\locale\language[installlanguagefallback]
Queries value: HKLM\system\currentcontrolset\control\mui\languages\en-us[type]
Queries value: HKLM\system\currentcontrolset\control\mui\languages\en-
us[alternatencodepage]
Queries value: HKCU\control panel\desktop[preferredlanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferredlanguages]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKLM\system\currentcontrolset\control\locale\sorting\versions[]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapisprivate]
Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
Queries value: HKLM\system\currentcontrolset\control\locale[en-us]
Queries value: HKLM\system\currentcontrolset\control\locale\extendedlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\locale[00000409]
Queries value: HKLM\system\currentcontrolset\control\locale\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\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid[
Queries value: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[
Queries value: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2)\inprocserver32[]
Queries value: HKCR\wow6432node\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\sqlclient\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\wow6432node\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\wow6432node\microsoft\windows\currentversion\internet settings[createuricachesize]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[enablepunycode]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[enablepunycode]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[enablepunycode]
Queries value: HKCU\software\microsoft\windows\currentversion\internet explorer\main\featurecontrol\feature_http_username_password_disable[62ddf7b757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\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\wow6432node\microsoft\internet explorer\main[frametabwindow]
Queries value: HKCU\software\microsoft\internet explorer\main[framemerging]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main[framemerging]
Queries value: HKCU\software\microsoft\internet explorer\main[sessionmerging]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main[sessionmerging]
Queries value: HKCU\software\microsoft\internet explorer\main[admintabprocs]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main[admintabprocs]
Queries value: HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main[tabprocgrowth]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main[navigationdelay]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[usedrophandler]
Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[queryforinfotip]
Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[hideondesktopperuser]
Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[nofilefolderjunction]
Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[pintonamespacetree]

Queries value: HKCR\wow6432node\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\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[loadwithoutcom]

Queries value: HKCU\software\microsoft\windows\currentversion\shellextensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d}] {000214e6-0000-0000-c000-000000000046; 0xffff}

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[]

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[threadingmodel]

Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nofilemenu]

Queries value: HKLM\software\microsoft\windows\currentversion\policies\ratings[key]

Queries value: HKCU\software\microsoft\windows\currentversion\internetsettings[urlencoding]

Queries value: HKLM\software\wow6432node\microsoft\internetexplorer\main\featurecontrol\feature_unc_savedfilecheck[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]

Queries value: HKLM\software\wow6432node\microsoft\internetexplorer\main\featurecontrol\feature_unc_savedfilecheck[*]

Queries value: HKLM\software\policies\microsoft\internetexplorer\security[disablesecuritysettingscheck]

Queries value: HKCU\software\microsoft\windows\currentversion\internetsettings\zones\0[flags]

Queries value: HKCU\software\microsoft\windows\currentversion\internetsettings\zones\1[flags]

Queries value: HKCU\software\microsoft\windows\currentversion\internetsettings\zones\2[flags]

Queries value: HKCU\software\microsoft\windows\currentversion\internetsettings\zones\3[flags]

Queries value: HKCU\software\microsoft\windows\currentversion\internetsettings\zones\4[flags]

Queries value: HKCU\software\microsoft\internetexplorer\main\featurecontrol\feature_localmachine_lockdown[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]

Queries value: HKCU\software\microsoft\internetexplorer\main\featurecontrol\feature_localmachine_lockdown[*]

Queries value: HKLM\software\wow6432node\microsoft\internetexplorer\main\featurecontrol\feature_localmachine_lockdown[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]

Queries value: HKLM\software\wow6432node\microsoft\internetexplorer\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\internetsettings[fromcachetimeout]

Queries value: HKLM\software\policies\microsoft\windows\currentversion\internetsettings[secureprotocols]

Queries value: HKCU\software\policies\microsoft\windows\currentversion\internetsettings[secureprotocols]

Queries value: HKCU\software\microsoft\windows\currentversion\internetsettings[secureprotocols]

Queries value: HKCU\software\microsoft\windows\currentversion\internetsettings[certificaterevocation]

Queries value: HKCU\software\microsoft\windows\currentversion\internetsettings[disablekeepalive]

Queries value: HKCU\software\microsoft\windows\currentversion\internetsettings[disablepassport]

Queries value: HKCU\software\microsoft\windows\currentversion\internetsettings[idnenabled]

Queries value: HKCU\software\microsoft\windows\currentversion\internetsettings[cachemode]

Queries value: HKLM\software\policies\microsoft\windows\currentversion\internetsettings[enablehttp1_1]

Queries value: HKCU\software\policies\microsoft\windows\currentversion\internetsettings[enablehttp1_1]

Queries value: HKCU\software\microsoft\windows\currentversion\internetsettings[enablehttp1_1]

Queries value: HKLM\software\policies\microsoft\windows\currentversion\internetsettings[proxyhttp1.1]

Queries value: HKCU\software\policies\microsoft\windows\currentversion\internetsettings[proxyhttp1.1]

Queries value: HKCU\software\microsoft\windows\currentversion\internetsettings[proxyhttp1.1]

Queries value: HKCU\software\microsoft\windows\currentversion\internetsettings[enablenegotiate]

Queries value: HKCU\software\microsoft\windows\currentversion\internetsettings[disablebasicoverclearchannel]

Queries value: HKCU\software\microsoft\internetexplorer\main\featurecontrol[feature_clientauthcertfilter]

Queries value: HKLM\software\wow6432node\microsoft\internetexplorer\main\featurecontrol[feature_clientauthcertfilter]

Queries value: HKCU\software\microsoft\windows\currentversion\internetsettings[clientauthbuiltinui]

Queries value: HKCU\software\microsoft\windows\currentversion\internetsettings[syncmode5]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internetsettings\5.0\cache[sessionstarttimedefaultdeltasecs]

Queries value: HKCU\software\microsoft\windows\currentversion\internetsettings\5.0\cache[signature]

Queries value: HKCU\software\microsoft\windows\currentversion\internetsettings\5.0\cache\content[peruseritem]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internetsettings\5.0\cache\content[peruseritem]

[illegible]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local appdata]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsiname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001[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[cache\limit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[parentfolder]
Queries value:

[illegible]

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

Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cache\limit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cache\options]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cache\repair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cache\path]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cache\prefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cache\limit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cache\options]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cache\repair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cache\path]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cache\prefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cache\limit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cache\options]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cache\repair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cache\path]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cache\prefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cache\limit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cache\options]
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[mcbsservername]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcscapiforcrack]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[utf8servernames]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[socketssendbufferlength]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connecttimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connectretries]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sendtimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[receptivetimeout]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[receptivetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmprauth]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]

Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[ftptdefaultexpirytimesecs]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttptnocachecheck]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasshttptnocachecheck]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocheck]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasssslnocheck]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[enablehttptrace]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrevving]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[tcpautotuning]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
Queries value:
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\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]

[illegible]

Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad[wpadoverride]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[nonetautodial]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[badproxyexpiretime]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disablebranchcache]
Queries value: HKLM\software\wow6432node\microsoft\tracing[enableconsoletracing]
Queries value: HKLM\software\wow6432node\microsoft\tracing\rasapi32[enablefiletracing]
Queries value: HKLM\software\wow6432node\microsoft\tracing\rasapi32[filetracingmask]
Queries value: HKLM\software\wow6432node\microsoft\tracing\rasapi32[enableconsoletracing]
Queries value: HKLM\software\wow6432node\microsoft\tracing\rasapi32[consoletracingmask]
Queries value: HKLM\software\wow6432node\microsoft\tracing\rasapi32[maxfilesize]
Queries value: HKLM\software\wow6432node\microsoft\tracing\rasapi32[filedirectory]
Queries value: HKLM\software\wow6432node\microsoft\tracing\rasmancs[enablefiletracing]
Queries value: HKLM\software\wow6432node\microsoft\tracing\rasmancs[filetracingmask]
HKLM\software\wow6432node\microsoft\tracing\rasmancs[enableconsoletracing]
Queries value: HKLM\software\wow6432node\microsoft\tracing\rasmancs[consoletracingmask]
Queries value: HKLM\software\wow6432node\microsoft\tracing\rasmancs[maxfilesize]
Queries value: HKLM\software\wow6432node\microsoft\tracing\rasmancs[filedirectory]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
Queries value: HKLM\software\microsoft\sqlclient\windows\disabledprocesses[2ac077a7]
Queries value:
HKLM\software\microsoft\sqlclient\windows\disabledsessions[machinethrottling]
Queries value:
HKLM\software\microsoft\sqlclient\windows\disabledsessions[globalsession]
Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxysettingsperuser]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
Queries value: HKLM\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[screndefaultservers]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[dynamicserverqueryorder]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[filterclusterip]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[waitfornameerroronall]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[usedns]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[dnssecurenamequeryfallback]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[enabledaforallnetworks]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[directaccessqueryorder]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[queryipmatching]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[usehostsfile]

Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[addrconfigcontrol]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registerprimaryname]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registerreverselookup]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registerwanadapters]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationttl]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressesstoregister]
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[updateopleveldomainzones]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[downcasespncauseapiowneristoolazy]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationoverwrite]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[maxcachesize]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[maxcachettl]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[maxnegativecachettl]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[adapertimeoutlimit]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[serverprioritytimelimit]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[maxcachedsockets]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[enablemulticast]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastresponderflags]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastsenderflags]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastsendermaxtimeout]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[dnstest]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[usecompartments]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[cacheallcompartments]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[usenewregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[resolverregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[resolverregistrationonly]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[dnsquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[dnsquickquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
Queries value: HKCU\software\microsoft\internet explorer[no3dborder]
Queries value: HKLM\software\wow6432node\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\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\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\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\user agent[]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[compatible]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\user agent[compatible]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[user

agent]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation[*]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[*]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[*]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableutf8]
Queries value: HKCU\software\microsoft\internet explorer\international[acceptlanguage]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_legacy_compression[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_legacy_compression[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1a10]
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\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
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\wow6432node\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
Queries value: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}[]
Queries value: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32[threadingmodel]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters\dnsCache[shutdownonidle]
Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[searchlist]
Queries value: HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}[]
Queries value: HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprocserver32[]
Queries value: HKCR\wow6432node\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[a]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\runmru[d]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\runmru[c]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\runmru[b]
Queries value: HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}[]
Queries value: HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprocserver32[threadingmodel]
Queries value: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}[]
Queries value: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32[threadingmodel]

Queries value: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32[]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete\client[]

Queries value: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\progid[]

Queries value: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}[]

Queries value: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\inprocserver32[threadingmodel]

Queries value: HKLM\software\microsoft\rpc\extensions\ndrolextdll]

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\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[enabledhcp]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[registrationenabled]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[registeradaptername]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[domain]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[dhcpdomain]

Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[dhcpv6domain]

Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[nameserver]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[nameserver]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[dhcpnameserver]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[enabledhcp]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registrationenabled]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registeradaptername]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[domain]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpdomain]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[nameserver]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpnameserver]

Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[queryadaptername]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[disableadapterdomainname]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[registrationmaxaddresscount]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[maxnumberofaddressesstoregister]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[enablemulticast]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[queryadaptername]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[disableadapterdomainname]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[disabledynamicupdate]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[enableadapterdomainnameregistration]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-

806e6f6e6963}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[maxnumberofaddressesstoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[enablemulticast]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
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\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[istextplainhonored]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_feeds[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_feeds[*]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[*]
Queries value: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[]
Queries value: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[]
Queries value: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[threadingmodel]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[*]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_object_caching[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\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\wow6432node\microsoft\internet explorer\application
compatibility[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.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[dragscrollldelay]
Queries value: HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinterval]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[*]
Queries value: HKCR\protocols\handler\about[clsid]
Queries value: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}[]
Queries value: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[threadingmodel]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\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\wow6432node\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\wow6432node\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[disablescripdebuggerie]
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\wow6432node\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\ntp\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\wow6432node\microsoft\internet explorer\version vector[vm1]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\version vector[windowsedition]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation[62ddfbbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation[*]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_xssfilter[62ddfbbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\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\wow6432node\microsoft\internet explorer\low rights[protectedmodeoffforallzones]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[icon]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\0[minlevel]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\0[recommendedlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[currentlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[icon]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\1[minlevel]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\1[recommendedlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[currentlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[2500]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\1[2500]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[icon]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\2[minlevel]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\2[recommendedlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[currentlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[2500]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\2[2500]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[icon]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\3[minlevel]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\3[recommendedlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[currentlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\zones\3[2500]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\zones\3[2500]
Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\zones\4[icon]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\zones\4[minlevel]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\zones\4[recommendedlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\zones\4[currentlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\zones\4[2500]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\zones\4[2500]
Queries value: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_mshtml_autoload_ieframe[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\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\wow6432node\microsoft\windows\currentversion\internet

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

explorer\main\featurecontrol\feature_subdownload_lockdown[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_subdownload_lockdown[*]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet

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

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

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

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

explorer\main\featurecontrol\feature_sslux[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\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: HKCU\software\microsoft\windows\currentversion\internet

settings[warnonintranet]
Queries value: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}[]

Queries value: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}\inprocserver32[threadingmodel]

Queries value: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}\progid[]

Queries value: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}[]

Queries value: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}\inprocserver32[threadingmodel]

Queries value: HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]

Queries value: HKLM\software\microsoft\ole[defaulttaccesspermission]

Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]

Queries value: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft_strong_cryptographic

provider[type]
Queries value: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft_strong_cryptographic

provider[image_path]
Queries value: HKLM\system\currentcontrolset\control\session

manager[safeprocesssearchmode]
Queries value: HKLM\system\currentcontrolset\control\lsa\lipsalgorithmpolicy[enabled]

Queries value: HKLM\system\currentcontrolset\control\lsa[lipsalgorithmpolicy]

Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]

Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]

Queries value: HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]

Queries value: HKLM\software\microsoft\cryptography[machineguid]

Queries value: HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32[]

Queries value: HKLM\software\microsoft\rpc\extensions[remoterpcdll]

Queries value: HKCU\software\microsoft\internet_explorer\recovery[autorecover]

Queries value: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_scripturl_mitigation[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_block_lmz_img[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet

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

explorer\main\featurecontrol\feature_behaviors[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_behaviors[*]
Queries value: HKLM\software\wow6432node\microsoft\internet_explorer\default

behaviors[homepage]
Queries value: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\progid[]

Queries value: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}[]

Queries value: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[threadingmodel]

Queries value: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\progid[]

Queries value: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}[]

Queries value: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32[threadingmodel]

Queries value: HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}[]

Queries value: HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserver32[threadingmodel]

Queries value: HKLM\software\wow6432node\microsoft\internet explorer\default behaviors[dxtfilterbehavior]

Queries value: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}[]

Queries value: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32[threadingmodel]

Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]

Queries value: HKLM\software\wow6432node\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\{43056cc8-3bf6-4ce7-bd67-1e1a187c13e9}\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\wow6432node\microsoft\directdraw\compatibility\bug![name]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\bug![flags]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\bug![id]

HKLM\software\wow6432node\microsoft\directdraw\compatibility\demolitionderby2[name]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\demolitionderby2[flags]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\demolitionderby2[id]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\diablo[name]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\diablo[flags]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\diablo[id]

HKLM\software\wow6432node\microsoft\directdraw\compatibility\mortalkombat3[name]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\mortalkombat3[flags]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\mortalkombat3[id]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\msgolf98[name]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\msgolf98[flags]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\msgolf98[id]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\nhlpowerplay[name]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\nhlpowerplay[flags]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\nhlpowerplay[id]

HKLM\software\wow6432node\microsoft\directdraw\compatibility\nortonsysteminfo[name]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\nortonsysteminfo[flags]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\nortonsysteminfo[id]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue squadron[name]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue squadron[flags]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue squadron[id]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\savage[name]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\savage[flags]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\savage[id]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\scorchedplanet[name]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\scorchedplanet[flags]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\scorchedplanet[id]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\silentthunder[name]

Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\silentthunder[flags]

```

Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\silentthunder[id]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft100[name]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft100[flags]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft100[id]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft115[name]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft115[flags]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft115[id]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraftdemo[name]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraftdemo[flags]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraftdemo[id]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\terraccide[name]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\terraccide[flags]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\terraccide[id]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\thirddimension[name]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\thirddimension[flags]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\thirddimension[id]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[name]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[flags]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[id]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[name]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[flags]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[id]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\modexonly[]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw[emulationonly]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw[showframerate]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw[enableprntscreen]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw[forceagpsupport]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw[disableagpsupport]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw[disablemmx]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw[disableddscapsinddsd]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw[disablewider surfaces]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw[usenonlocalvidmem]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw[forcerefreshrate]
Queries value:
HKLM\software\wow6432node\microsoft\direct3d[flipnovsync]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw[owndc]
Queries value:
HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\progid[]
Queries value:
HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}[]
Queries value:
HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32[inprocserver32]
Queries value:
HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32[]
Queries value:
HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32[threadingmodel]
Queries value:
HKCR\dximagettransform.microsoft.shadow\clsid[]
Queries value:
HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\progid[]
Queries value:
HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}[]
Queries value:
HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprocserver32[inprocserver32]
Queries value:
HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprocserver32[]
Queries value:
HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprocserver32[threadingmodel]
Queries value:
HKCR\mime\databse\content type\image/png[extension]
Queries value:
HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\progid[]
Queries value:
HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}[]
Queries value:
HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[inprocserver32]
Queries value:
HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[]
Queries value:
HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[threadingmodel]
Queries value:
HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\progid[]
Queries value:
HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}[]
Queries value:
HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32[inprocserver32]
Queries value:
HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32[]
Queries value:
HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32[threadingmodel]
Queries value:
HKCR\mime\databse\content type\image/bmp/bits[0]
Queries value:
HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}[]
Queries value:
HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32[inprocserver32]
Queries value:
HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32[]
Queries value:
HKCR\mime\databse\content type\image/gif/bits[0]
Queries value:
HKCR\mime\databse\content type\image/jpeg/bits[0]
Queries value:
HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32[threadingmodel]
Queries value:
HKCR\mime\databse\content type\image/pipeg/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\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\progid[]
Queries value: HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}[]
Queries value: HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[threadingmodel]
Queries value: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\progid[]
Queries value: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}[]
Queries value: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32[]
Queries value: HKCR\wow6432node\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\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}[]
Queries value: HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32[threadingmodel]
Queries value: HKLM\system\currentcontrolset\control\clsid\codepage[1250]
Queries value: HKLM\system\currentcontrolset\control\clsid\codepage[1251]
Queries value: HKLM\system\currentcontrolset\control\clsid\codepage[1253]
Queries value: HKLM\system\currentcontrolset\control\clsid\codepage[1254]
Queries value: HKLM\system\currentcontrolset\control\clsid\codepage[1255]
Queries value: HKLM\system\currentcontrolset\control\clsid\codepage[1256]
Queries value: HKLM\system\currentcontrolset\control\clsid\codepage[1257]
Queries value: HKLM\system\currentcontrolset\control\clsid\codepage[1258]
Queries value: HKLM\system\currentcontrolset\control\clsid\codepage[874]
Queries value: HKLM\system\currentcontrolset\control\clsid\codepage[932]
Queries value: HKLM\system\currentcontrolset\control\clsid\codepage[936]
Queries value: HKLM\system\currentcontrolset\control\clsid\codepage[949]
Queries value: HKLM\system\currentcontrolset\control\clsid\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: HKCR\mime\database\content type\image/gif[extension]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_block_lmz_script[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_block_lmz_script[*]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_use_windowedselectcontrol[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_use_windowedselectcontrol[*]
Queries value: HKCU\software\microsoft\windows script\settings[jitdebug]
Queries value: HKCU\software\microsoft\internet explorer\new windows[accuserinonlick]
Queries value: HKLM\software\wow6432node\microsoft\direct3d[disablemmx]
Queries value: HKLM\software\wow6432node\microsoft\direct3d[disablex3d]
Queries value: HKLM\software\wow6432node\microsoft\direct3d[fewvertices]
Queries value: HKLM\software\wow6432node\microsoft\direct3d[disablevidmemvbs]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\simsum[plane1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\simsum[plane2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\simsum[plane3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\simsum[plane4]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\simsum[plane5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\simsum[plane6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\simsum[plane7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\simsum[plane8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\simsum[plane9]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\simsum[plane10]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\simsum[plane11]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\simsum[plane12]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\simsum[plane13]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\simsum[plane14]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\simsum[plane15]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\simsum[plane16]
Queries value: HKCR\wow6432node\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid32[]
Queries value: HKCR\wow6432node\interface\{332c4425-26cb-11d0-b483-00c04fd90119}\proxystubclsid32[]

Queries value: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}[]
Queries value: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32[threadingmodel]
Queries value: HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32[]
Queries value: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32[]
Queries value: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[]
Queries value: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[threadingmodel]
Queries value: HKCR\shockwaveflash.shockwaveflash\clsid[]
Queries value: HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\progid[]
Queries value: HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}[]
Queries value: HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprocserver32[]
Queries value: HKCR\wow6432node\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: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider types\type 001[name]
Queries value: HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\1.0\0\win32[]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\default behaviors[userdata]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_activex_repurposedetection[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_activex_repurposedetection[*]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_addon_management[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_addon_management[*]
Queries value: HKCR\wow6432node\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\miscstatus\1[]
Queries value: HKLM\software\wow6432node\microsoft\windows\tablet_pc[istabletpc]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[2000]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\feed discovery[sound]
Queries value: HKCU\software\microsoft\ftp[use web based ftp]
Queries value: HKCR\mime\database\content_type\application/x-shockwave-flash[extension]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32[wave]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32[wave1]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32[wave2]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32[wave3]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32[wave4]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32[wave5]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32[wave6]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32[wave7]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32[wave8]
Queries value: HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\progid[]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32[wave9]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32[midi]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32[midi1]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32[midi2]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32[midi3]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32[midi4]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32[midi5]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32[midi6]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32[midi7]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32[midi8]
Queries value: HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}[]
Queries value: HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprocserver32[inprocserver32]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32[midi9]
Queries value: HKCU\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
Queries value: HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprocserver32[threadingmodel]

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[cache\repair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cache\path]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cache\prefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cache\limit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cache\options]
Queries value:
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignedll]
Queries value:
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignature\routine]
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: HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}[]
Queries value: HKCU\software\microsoft\internet explorer\domstorage\baidu.com[]
Queries value: HKCU\software\macromedia\flashplayer[flashplayer\version]
Queries value: HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\proxystubclsid32[]
Queries value: HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\typelib[]
Queries value: HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\typelib[version]
Queries value: HKCU\software\microsoft\internet
explorer\services[selectionactivitybutton\disable]
Queries value: HKCU\software\microsoft\internet explorer\suggested sites[enabled]
Queries value: HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32[]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[usedrophandler]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsparsedisplayname]
Queries value: HKLM\software\microsoft\rpc[udtalignmentpolicy]
Queries value: HKCR\wow6432node\interface\{00020400-0000-0000-c000-
000000000046}\proxystubclsid32[]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforinfotip]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideondesktop\topperuser]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[no\file\folder\junction]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[pintonamespacetree]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hasnavigationenum]
Queries value: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}[]
Queries value: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32[]
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\{8063a3d4-8213-
11e3-a68e-806e6f6e6963}[data]
Queries value: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d4-8213-
11e3-a68e-806e6f6e6963}[generation]

Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-11e3-a68e-806e6f6e963}[data]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-11e3-a68e-806e6f6e963}[generation]
Queries value: HKCR\wow6432node\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32[]
Queries value: HKCR\drive\shellex\folderextensions\{fbef8a05-beee-4442-804e-409d6c4515e9}[drivemask]
Queries value: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}[]
Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
Queries value: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[threadingmodel]
Queries value: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[threadingmodel]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
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[icononly]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
Queries value: HKCR\wow6432node\interface\{00020404-0000-0000-c000-000000000046}\proxystubclsid32[]
Queries value: HKCR\directory[docobject]
Queries value: HKCR\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}[]
Queries value: HKCR\folder[docobject]
Queries value: HKCR\allfilesystemobjects[docobject]
Queries value: HKCR\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}\inprocserver32[]
Queries value: HKCR\directory[browseinplace]
Queries value: HKCR\folder[browseinplace]
Queries value: HKCR\allfilesystemobjects[browseinplace]
Queries value: HKCR\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}\inprocserver32[threadingmodel]
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\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32[loadwithoutcom]
Queries value: HKCU\software\microsoft\windows\currentversion\shellextensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {000214e6-0000-0000-c000-000000000046} 0xffff]
Queries value: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[]
Queries value: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016040820160409[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\extensible cache\mshist012016040820160409[cacheopath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016040820160409[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016040820160409[cacheimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016040820160409[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[localizedstring]
Queries value: HKCU\software\microsoft\internet
explorer\main\windowssearch[enabledscopes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[parsiname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[favorites]
Queries value: HKLM\software\wow6432node\microsoft\windows search[currentversion]
Queries value: HKLM\software\wow6432node\microsoft\downloadmanager[cacheok]
Queries value: HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\progid[]
Queries value: HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}[]
Queries value: HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprocserver32[threadingmodel]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main[maxrenderline]
Queries value: HKCR\mime\database\content type\image/x-icon[extension]
Queries value: HKCR\shockwaveflash.shockwaveflash.7\clsid[]
Queries value: HKCU\appevents\schemes\apps\explorer\navigating\current[]
Queries value: HKCU\appevents\schemes[]
Queries value: HKCU\appevents\schemes\apps\explorer\navigating\current[default flags]
Queries value: HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}[]
Queries value: HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32[threadingmodel]
Queries value: HKCU\appevents\schemes\apps\explorer\activatingdocument\current[]
Queries value: HKCR\mime\database\content type\image/jpeg[extension]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\default

```
behaviors[clientcaps]
  Queries value: HKCR\msxml2.xmlhttp\clsid[]
  Queries value: HKCR\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\progid[]
  Queries value: HKCR\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}[]
  Queries value: HKCR\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\inprocserver32[inprocserver32]
  Queries value: HKCR\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\inprocserver32[]
  Queries value: HKCR\wow6432node\clsid\{f6d90f16-9c73-11d3-b32e-00c04f990bb4}\inprocserver32[threadingmodel]
  Queries value: HKCR\shockwaveflash.shockwaveflash.10\clsid[]
  Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_block_lmz_object[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
  Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_block_lmz_object[*]
  Queries value: HKCR\swf[content type]
  Queries value: HKCR\mime\database\content type\application/x-shockwave-flash[clsid]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1c00]
  Queries value: HKCR\acropdf.pdf.1\clsid[]
  Queries value: HKCR\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-444553540000}\progid[]
  Queries value: HKCR\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-444553540000}[]
  Queries value: HKCR\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-444553540000}\inprocserver32[inprocserver32]
  Queries value: HKCR\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-444553540000}\inprocserver32[]
  Queries value: HKCR\wow6432node\clsid\{ca8a9780-280d-11cf-a24d-444553540000}\inprocserver32[threadingmodel]
  Queries value: HKCU\software\adobe\acrobat reader\9.0\originals[browserintegration]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{08b0e5c0-4fcb-11cf-aaa5-00401c608500}[isinstalled]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{08b0e5c0-4fcb-11cf-aaa5-00401c608500}[version]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{08b0e5c0-4fcb-11cf-aaa5-00401c608500}[keyfilename]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{22d6f312-b0f6-11d0-94ab-0080c74c7e95}[isinstalled]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{22d6f312-b0f6-11d0-94ab-0080c74c7e95}[version]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{22d6f312-b0f6-11d0-94ab-0080c74c7e95}[keyfilename]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{3af36230-a269-11d1-b5bf-0000f8051515}[isinstalled]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{3af36230-a269-11d1-b5bf-0000f8051515}[version]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{3af36230-a269-11d1-b5bf-0000f8051515}[keyfilename]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{44bba840-cc51-11cf-aafa-00aa00b6015c}[isinstalled]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{44bba840-cc51-11cf-aafa-00aa00b6015c}[version]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{44bba840-cc51-11cf-aafa-00aa00b6015c}[keyfilename]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{45ea75a0-a269-11d1-b5bf-0000f8051515}[isinstalled]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{45ea75a0-a269-11d1-b5bf-0000f8051515}[version]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{45ea75a0-a269-11d1-b5bf-0000f8051515}[keyfilename]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{7790769c-0471-11d2-af11-00c04fa35d02}[isinstalled]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{7790769c-0471-11d2-af11-00c04fa35d02}[version]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{7790769c-0471-11d2-af11-00c04fa35d02}[keyfilename]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{89820200-ecbd-11cf-8b85-00aa005b4340}[isinstalled]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{89820200-ecbd-11cf-8b85-00aa005b4340}[version]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{89820200-ecbd-11cf-8b85-00aa005b4340}[keyfilename]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{89820200-ecbd-11cf-8b85-00aa005b4383}[isinstalled]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{89820200-ecbd-11cf-8b85-00aa005b4383}[version]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{89820200-ecbd-11cf-8b85-00aa005b4383}[keyfilename]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{9381d8f2-0288-11d0-9501-00aa00b911a5}[isinstalled]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{9381d8f2-0288-11d0-9501-00aa00b911a5}[version]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{9381d8f2-0288-11d0-9501-00aa00b911a5}[keyfilename]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{de5aed00-a4bf-11d1-9948-00c04f98bbc9}[isinstalled]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{de5aed00-a4bf-11d1-9948-00c04f98bbc9}[version]
  Queries value: HKLM\software\wow6432node\microsoft\active setup\installed components\{de5aed00-a4bf-11d1-9948-00c04f98bbc9}[keyfilename]
  Sets/Creates value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_scripturl_mitigation[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
  Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\rasapi32[enablefiletracing]
  Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\rasapi32[enableconsoletracing]
  Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\rasapi32[filetracingmask]
  Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\rasapi32[consoletracingmask]
  Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\rasapi32[maxfilesize]
  Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\rasapi32[filedirectory]
  Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\rasmancs[enablefiletracing]
  Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\rasmancs[enableconsoletracing]
  Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\rasmancs[filetracingmask]
```

Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\rasmancs[consoletracingmask]
Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\rasmancs[maxfilesize]
Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\rasmancs[filedirectory]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cacheopath]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cacheoprefix]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cacheolimit]
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\mshist012016040820160409[cacheopath]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016040820160409[cacheoprefix]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016040820160409[cacheolimit]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016040820160409[cacheoptions]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016040820160409[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:
HKLM\software\wow6432node\microsoft\directdraw\mostrecentapplication[name]
Value changes: HKLM\software\wow6432node\microsoft\directdraw\mostrecentapplication[id]
Value changes: HKLM\software\wow6432node\microsoft\direct3d\mostrecentapplication[name]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cacheopath]
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\mshist012016040820160409[cacheopath]
Value changes: HKCU\software\microsoft\internet explorer\main\windowssearch[version]