Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 54, Task ID: 205

Task ID: 205 Risk Level:

Date Processed: 2016-04-22 06:01:56 (UTC)

Processing Time: 61.11 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\1af5338669efabe0a9841478396871b1.exe"

Sample ID: Type: basic admin Owner:

1af5338669efabe0a9841478396871b1 Label:

2016-04-22 06:01:55 (UTC) Date Added:

PE32:win32:gui File Type: File Size: 939520 bytes

1af5338669efabe0a9841478396871b1 MD5:

98511820966946e5c2c543c720816047a808816f674bc8525016f362785c8b3e SHA256:

Description: None

Pattern Matching Results

Creates malicious events: FakelE [PUA , Downware]

2 ECMA Script

3 Connects to local host

3 HTTP connection - response code 200 (success)

3 Long sleep detected

4 Checks whether debugger is present

2 HTML file 1 YARA score 1

Static Events

YARA rule hit: SWF

YARA rule hit: Nonexecutable

Process/Thread Events

C:\WINDOWS\Temp\1af5338669efabe0a9841478396871b1.exe Creates process:

["c:\windows\temp\1af5338669efabe0a9841478396871b1.exe"]

Loads service: RASMAN [C:\WINDOWS\system32\svchost.exe -k netsvcs]

Named Object Events

Creates mutex: \BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003

Creates mutex:

\BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-

507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003 $\verb|\BaseNamedObjects\c:!documents| and settings! admin! local \\$ Creates mutex:

settings!temporary internet files!content.ie5!

\BaseNamedObjects\c:!documents and settings!admin!cookies! Creates mutex: \BaseNamedObjects\c:!documents and settings!admin!local Creates mutex:

settings!history!history.ie5!

\BaseNamedObjects\WininetConnectionMutex Creates mutex:

\BaseNamedObjects\ZonesCounterMutex Creates mutex:

\BaseNamedObjects\ZoneAttributeCacheCounterMutex Creates mutex:

Creates mutex: \BaseNamedObjects\ZonesCacheCounterMutex \BaseNamedObjects\ZonesLockedCacheCounterMutex Creates mutex: Creates mutex: \BaseNamedObjects\MSCTF.Shared.MUTEX.EJ

Creates mutex: **\BaseNamedObjects\!PrivacIE!SharedMemory!Mutex** Creates mutex: \BaseNamedObjects\DDrawWindowListMutex

\BaseNamedObjects\DDrawDriverObjectListMutex Creates mutex: Creates mutex: \BaseNamedObjects__DDrawExclMode_ \BaseNamedObjects__DDrawCheckExclMode_ Creates mutex: \BaseNamedObjects\MSCTF.Shared.MUTEX.MHC Creates mutex:

Creates mutex: \BaseNamedObjects\DirectSound DllMain mutex (0x0000010C) Creates mutex: \BaseNamedObjects\{1B655094-FE2A-433c-A877-FF9793445069}

\BaseNamedObjects\http://www.baidu.com/ Creates mutex:

Creates mutex: \BaseNamedObjects\c:!documents and settings!admin!local

settings!application data!microsoft!internet explorer!domstore!

\BaseNamedObjects\c:!documents and settings!admin!application Creates mutex:

data!microsoft!internet explorer!userdata!

Creates mutex: \BaseNamedObjects\InternetExplorerDOMStoreQuota

\BaseNamedObjects_!SHMSFTHISTORY!_ Creates mutex:

\BaseNamedObjects\c:!documents and settings!admin!local Creates mutex:

settings!history!history.ie5!mshist012016042220160423!

\BaseNamedObjects\MSIMGSIZECacheMutex Creates mutex:

\BaseNamedObjects\usereny: User Profile setup event Creates event: Creates event: \BaseNamedObjects\MSCTF.SendReceive.Event.MHC.IC \BaseNamedObjects\MSCTF.SendReceiveConection.Event.MHC.IC Creates event: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1} Creates semaphore: Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}

File System Events

Creates semaphore:

C:\Documents and Settings\Admin\Cookies\admin@baidu[1].txt Creates Creates: C:\Documents and Settings\Admin\Cookies\admin@baidu[21.txt

Creates C:\Documents and Settings\Admin\Local Settings\Temporary Internet

\BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}

Files\Content.IE5\QXMNQBKF\index[1].php

C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates:

Files\Content.IE5\CXCXW1MR\baidu_jgylogo3[1].gif

C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates:

Files\Content.IE5\QXMNQBKF\jquery-1.10.2.min_f2fb5194[1].js

Creates C:\Documents and Settings\Admin\Local Settings\Temporary Internet

Files\Content.IE5\QXMNQBKF\bd_logo1[1].png

C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates:

Files\Content.IE5\UH4D6D6X\nuomi_510f7472[1].png

C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates:

Files\Content.IE5\CXCXW1MR\icons_0e814c16[1].png

Creates C:\Documents and Settings\Admin\Local Settings\Temporary Internet

Files\Content.IE5\UH4D6D6X\zbios_62c636fe[1].png

C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates:

Files\Content.IE5\CXCXW1MR\all_async_search_641293e1[1].js

C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates:

Files\Content.IE5\CXCXW1MR\every_cookie_aa168cb4[1].js

C:\Documents and Settings\Admin\Local Settings\Application

Data\Microsoft\Internet Explorer\DOMStore\3FDD734T\www.baidu[1].xml

C:\Documents and Settings\Admin\Cookies\admin@www.baidu[1].txt Creates: Creates: C:\Documents and Settings\Admin\Cookies\admin@www.baidu[2].txt C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates: Files\Content.IE5\QXMNQBKF\quickdelete_9c14b01a[1].png

Creates

C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\env_beb83b45[1].swf

C:\Documents and Settings\Admin\Application Data\Microsoft\Internet Creates:

Explorer\UserData C:\Documents and Settings\Admin\Application Data\Microsoft\Internet Creates:

Explorer\UserData\index.dat

Creates: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet

Explorer\UserData\Z2XJ2MAQ

C:\Documents and Settings\Admin\Application Data\Microsoft\Internet Creates:

Explorer\UserData\2LA1AXWL

Creates: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet

Explorer\UserData\009WN0B0

Creates: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet

Explorer\UserData\B910PRFD

 ${\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}$ Creates:

Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com

C:\Documents and Settings\Admin\Application Data\Macromedia\Flash Creates:

Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx

Creates: C:\Documents and Settings\Admin\Application Data\Macromedia\Flash

Player\macromedia.com\support\flashplayer\sys\settings.sxx

C:\Documents and Settings\Admin\Application Data\Macromedia\Flash Creates:

Player\#SharedObjects\45PY3TTW\s1.bdstatic.com Creates:

C:\Documents and Settings\Admin\Application Data\Macromedia\Flash Player\#SharedObjects\45PY3TTW\s1.bdstatic.com\sharedObjectBIDUPSID.sxx

C:\Documents and Settings\Admin\Application Data\Microsoft\Internet

Explorer\UserData\Z2XJ2MAQ\userDataBIDUPSID[1].xml

C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates:

Files\Content.IE5\UH4D6D6X\bdsug_async_dac7ea02[1].js

C:\Documents and Settings\Admin\Local Creates

Settings\History\History.IE5\MSHist012016042220160423

C:\Documents and Settings\Admin\Local

Settings\History\History.IE5\MSHist012016042220160423\index.dat

C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates:

Files\Content.IE5\QXMNQBKF\baiduia_b45d552b[1].js C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates:

Files\Content.IE5\ONWV4FIP\JSocket_9a52fc3e[1].swf

C:\Documents and Settings\Admin\Local Settings\Temporary Internet

Files\Content.IE5\UH4D6D6X\favicon[1].ico

C:\Documents and Settings\Admin\Local Creates:

Settings\Temp\httpwww.baidu.comfavicon.ico

C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates:

Files\Content.IE5\CXCXW1MR\union[1].gif

C:\Documents and Settings\Admin\Local Settings\Temporary Internet

Files\Content.IE5\QXMNQBKF\nu_instant_search_ebeb5baa[1].js

```
C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\ONWV4FIP\bdbri_icons_2e35e84b[1].png
                         \hbox{\tt C:\WINDOWS\Prefetch\1AF5338669EFABE0A984147839687-1A3B3BCE.pf}
 Opens:
                         C:\Documents and Settings\Admin
 Opens:
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
 Opens:
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
 Opens:
                         C:\WINDOWS\system32\msimg32.dll
                         C:\WINDOWS\system32\ws2_32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\ws2help.dll
 Opens:
                         C:\WINDOWS\system32\psapi.dll
 Opens:
                         C:\WINDOWS\system32\imm32.dll
 Opens:
                         C:\WINDOWS\system32\shell32.dll
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Manifest
                         C:\WINDOWS\system32\SHELL32.dll.124.Config
 Opens:
 Opens:
                         C:\WINDOWS\WindowsShell.Manifest
 Opens:
                         C:\WINDOWS\WindowsShell.Config
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Config
 Opens:
                         C:\program files\fve31bb\zxz63d\Log.dat
 Opens:
                         C:\WINDOWS\system32\rpcss.dll
 Opens:
                         C:\WINDOWS\system32\MSCTF.dll
 Opens:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\restart.dat
 Opens:
                         C:\WINDOWS\system32\uxtheme.dll
 Opens:
                         C:\WINDOWS\system32\MSCTFIME.IME
 Opens:
                         C:\program files\fve31bb\zxz63d\log.dat
 Opens:
                         C:\WINDOWS\system32\clbcatq.dll
                         C:\WINDOWS\system32\comres.dll
 Opens:
 Opens:
                         C:\WINDOWS\Registration\R00000000007.clb
 Opens:
                         C:\WINDOWS\system32\ieframe.dll
                         C:\Program Files\Internet Explorer\iexplore.exe
 Opens:
 Opens:
                         C:\WINDOWS\system32\ieframe.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\ieframe.dll.123.Config
 Opens:
                         C:\WINDOWS\system32\en-US\ieframe.dll.mui
 Opens:
                         C:\WINDOWS\Temp\1af5338669efabe0a9841478396871b1.exe
 Opens:
                         C:\WINDOWS\system32\MSIMTF.dll
 Opens:
                         C:\WINDOWS\Temp\MJPGC.TMP
 Opens:
                         C:\WINDOWS\system32\WININET.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\WININET.dll.123.Config
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5
                         C:\Documents and Settings\Admin\Local Settings\History
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History\History.IE5
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Cookies
 Opens:
                         C:\Documents and Settings\Admin\Cookies\index.dat
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\index.dat
                         C:\WINDOWS\system32\rasapi32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\rasman.dll
 Opens:
                         C:\WINDOWS\system32\netapi32.dll
 Opens:
                         C:\WINDOWS\system32\tapi32.dll
 Opens:
                         C:\WINDOWS\system32\rtutils.dll
 Opens:
                         C:\WINDOWS\system32\winmm.dll
 Opens:
                         C:\WINDOWS\system32\TAPI32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\TAPI32.dll.124.Config
 Opens:
                         C:\AUTOEXEC.BAT
 Opens:
                         C:\
 Opens:
                         C:\Documents and Settings\All Users\Application
Data\Microsoft\Network\Connections\Pbk
 Opens:
                         C:\WINDOWS\system32\ras
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Microsoft\Network\Connections\Pbk\
 Opens:
                         C:\WINDOWS\system32\sensapi.dll
                         C:\WINDOWS\system32\mswsock.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\mlang.dll
 Opens:
                         C:\WINDOWS\system32\MLANG.dll.123.Manifest
                         C:\WINDOWS\system32\MLANG.dll.123.Config
 Opens:
 Opens:
                         C:\WINDOWS\system32\hnetcfg.dll
 Opens:
                         C:\WINDOWS\system32\wshtcpip.dll
 Opens:
                         C:\WINDOWS\system32\browseui.dll
 Opens:
                         C:\WINDOWS\system32\browseui.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\browseui.dll.123.Config
 Opens:
                         C:\WINDOWS\system32\msv1_0.dl1
 Opens:
                         C:\WINDOWS\system32\iphlpapi.dll
 Opens:
                         C:\WINDOWS\system32\rasadhlp.dll
 Opens:
                         C:\WINDOWS\system32\dnsapi.dll
 Opens:
                         C:\WINDOWS\system32\drivers\etc\hosts
 Opens:
                         C:\WINDOWS\system32\rsaenh.dll
 Opens:
                         C:\WINDOWS\system32\crypt32.dll
```

```
C:\Documents and Settings\Admin\Cookies\admin@baidu[1].txt
   Opens:
                                                   C:\Documents and Settings\Admin\Cookies\admin@baidu[2].txt
   Opens:
                                                   C:\WINDOWS\Temp\31eb3824-5e13-4a4d-b9c3-b0a7a5f07837
   Opens:
                                                   C:\WINDOWS\system32\mshtml.dll
   Opens:
   Opens:
                                                   C:\WINDOWS\system32\msls31.dll
   Opens:
                                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\index[1].php
                                                   C:\WINDOWS\system32\iepeers.dll
   Opens:
   Opens:
                                                   C:\WINDOWS\system32\winspool.drv
                                                   C:\WINDOWS\system32\iepeers.dll.123.Manifest
   Opens:
   Opens:
                                                   C:\WINDOWS\system32\iepeers.dll.123.Config
   Opens:
                                                   C:\WINDOWS\system32\jscript.dll
   Opens:
                                                   C:\WINDOWS\system32\winlogon.exe
                                                   C:\WINDOWS\system32\xpsp2res.dll
   Opens:
   Opens:
                                                   C:\WINDOWS\system32\dxtrans.dll
   Opens:
                                                   C:\WINDOWS\system32\atl.dll
   Opens:
                                                   C:\WINDOWS\system32\ddrawex.dll
   Opens:
                                                   C:\WINDOWS\system32\ddraw.dll
   Opens:
                                                   C:\WINDOWS\system32\dciman32.dll
                                                   C:\WINDOWS\win.ini
   Opens:
   Opens:
                                                   C:\WINDOWS\system32\dxtmsft.dll
   Opens:
                                                   C:\WINDOWS\system32\sxs.dll
   Opens:
                                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\jquery-1.10.2.min_f2fb5194[1].js
   Opens:
                                                   C:\WINDOWS\system32\imgutil.dll
   Opens:
                                                   C:\WINDOWS\Fonts\arialbd.ttf
   Opens:
                                                   C:\WINDOWS\Fonts\ariali.ttf
   Opens:
                                                   C:\WINDOWS\system32\pngfilt.dll
   Opens:
C: \verb|WINDOWS| \verb|WinSxS| x86_Microsoft. \verb|Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-ww_dfb54e0c| and the second s
   Opens:
\label{lem:c:windows.gdiPlus_6595b64144ccf1df_1.0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512\_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5512_x-0.2600.5
ww_dfb54e0c\GdiPlus.dll
   Opens:
                                                   C:\WINDOWS\system32\d3dim700.dll
                                                   C:\WINDOWS\system32\en-US\mshtml.dll.mui
   Opens:
   Opens:
                                                   C:\WINDOWS\system32\en-US\jscript.dll.mui
   Opens:
                                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\all_async_search_641293e1[1].js
                                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\every_cookie_aa168cb4[1].js
                                                   {\tt C:\WINDOWS\system32\Macromed\Flash\Flash10h.ocx}
   Opens:
   Opens:
                                                   \label{lem:c:windows} $$C:\WINDOWS\system 32\Macromed\Flash\Flash 10h.ocx. 2. Manifest
   Opens:
                                                   C:\WINDOWS\system32\Macromed\Flash\Flash10h.ocx.2.Config
   Opens:
                                                   C:\WINDOWS\system32\msasn1.dll
   Opens:
                                                   C:\WINDOWS\system32\dsound.dll
   Opens:
                                                   C:\WINDOWS\system32\mscms.dll
   Opens:
                                                   C: \verb|\WINDOWS\system32\Macromed\Flash\ss.sgn|
   Opens:
                                                   C:\WINDOWS\system32\Macromed\Flash
                                                   C:\WINDOWS\system32\Macromed\Flash\ss.cfg
   Opens:
   Opens:
                                                   C:\WINDOWS\system32\Macromed\Flash\mms.cfg
   Opens:
                                                   C:\WINDOWS\system32\Macromed\Flash\oem.cfg
   Opens:
                                                   C:\WINDOWS\system32\oem.cfg
   Opens:
                                                   C:\Documents and Settings\Admin\Application Data\Adobe\Flash
Player\AssetCache
   Opens:
                                                   C:\Documents and Settings\Admin\Application Data\Adobe\Flash Player
   Opens:
                                                   C:\WINDOWS\system32\stdole2.tlb
                                                   C:\Documents and Settings\Admin\Local Settings\Application
   Opens:
Data\Microsoft\Internet Explorer\DOMStore
                                                   C:\Documents and Settings\Admin\Local Settings\Application
   Opens:
Data\Microsoft\Internet Explorer\DOMStore\index.dat
   Opens:
                                                   C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\3FDD734T
                                                   C:\WINDOWS\system32\xmllite.dll
                                                   C:\Documents and Settings\Admin\Local Settings\Application
   Opens:
Data\Microsoft\Internet Explorer\DOMStore\3FDD734T\www.baidu[1].xml
                                                   C:\WINDOWS\system32\mshtml.tlb
   Opens:
   Opens:
                                                   C:\Documents and Settings\Admin\Cookies\admin@www.baidu[1].txt
   Opens:
                                                   \label{lem:cokies-admin@www.baidu[2].txt} C:\Documents\ and\ Settings\Admin\Cookies\admin@www.baidu[2].txt
   Opens:
                                                   C:\WINDOWS
                                                   C:\WINDOWS\system32
   Opens:
                                                   C:\Documents and Settings\Admin\Local Settings\Temporary Internet
   Opens:
Files\Content.IE5\ONWV4FIP\env_beb83b45[1].swf
   Opens:
                                                   C:\WINDOWS\system32\msxm13.dll
   Opens:
                                                   C:\WINDOWS\system32\msxml3r.dll
   Opens:
                                                   C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\UserData
   Opens:
                                                   C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\UserData\Z2XJ2MAQ
   Opens:
                                                   C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\UserData\2LA1AXWL
   Opens:
                                                   C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\UserData\0Q9WN0B0
   Opens:
                                                   C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
```

```
Explorer\UserData\B910PRFD
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\UserData\index.dat
 Opens:
                          C:\WINDOWS\system32\schannel.dll
                          C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
 Opens:
Player\#SharedObjects
                          C:\Documents and Settings\Admin\Application Data\Macromedia\Flash Player
 Opens:
                          C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
 Opens:
Player\#SharedObjects\45PY3TTW\macromedia.com\support\flashplayer\sys\settings.sol
                          C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\#SharedObjects\45PY3TTW\macromedia.com\support\flashplayer\sys\
 Opens:
                          {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
Player\macromedia.com\support\flashplayer\sys\settings.sol
                          C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
 Opens:
Player\#SharedObjects\45PY3TTW\s1.bdstatic.com\sharedObjectBIDUPSID.sol
                          C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
 Opens:
Player\#SharedObjects\45PY3TTW\s1.bdstatic.com\
 Opens:
                          {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
Player\s1.bdstatic.com\sharedObjectBIDUPSID.sol
 Opens:
                          {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
Player\s1.bdstatic.com\
 Opens:
                          C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\#SharedObjects\45PY3TTW\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sol
 Opens:
                          C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\#SharedObjects\45PY3TTW\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\
                          C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
 Opens:
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sol
 Opens:
                          C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\
 Opens:
                          C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com
                         C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
 Opens:
Player\macromedia.com\support\flashplayer\sys
 Opens:
                          C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer
 Opens:
                          C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
                          C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
 Opens:
Player\macromedia.com\support\flashplayer\sys\settings.sxx
 Opens:
                          C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\#SharedObjects\45PY3TTW\s1.bdstatic.com
 Opens:
                          C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\#SharedObjects\45PY3TTW
                          {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}
 Opens:
Player\#SharedObjects\45PY3TTW\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
 Opens:
                          C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
{\tt Explorer \backslash UserData \backslash Z2XJ2MAQ \backslash userDataBIDUPSID[1].xml}
 Opens:
                          C:\WINDOWS\system32\setupapi.dll
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\bdsug_async_dac7ea02[1].js
                          C:\Documents and Settings
                          C:\Documents and Settings\Admin\Local Settings
 Opens:
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
 Opens:
                          C:\WINDOWS\system32\actxprxy.dll
 Opens:
                          C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014033120140407
                          C:\Documents and Settings\Admin\Local
 Opens:
Settings \verb|\History\History\IE5\MSHist012014033120140407\verb|\Lindex.dat| \\
                          C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\MSHist012014041220140413
 Opens:
                          C:\Documents and Settings\Admin\Local
Settings \verb|\History\E5| MSH is to 12014041220140413 \verb|\index.dat| \\
                          C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012016042220160423
                          C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\MSHist012016042220160423\index.dat
 Opens:
                          C:\DOCUME~1\Admin\LOCALS~1\Temp\httpwww.baidu.comfavicon.ico
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\baiduia_b45d552b[1].js
                          C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\JSocket 9a52fc3e[1].swf
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\favicon[1].ico
                          C:\Documents and Settings\Admin\Local Settings\Temp
 Opens:
 Opens:
                          C:\Documents and Settings\Admin\Local
Settings\Temp\httpwww.baidu.comfavicon.ico
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\nu_instant_search_ebeb5baa[1].js
 Writes to:
                          C:\Documents and Settings\Admin\Cookies\admin@baidu[1].txt
                          C:\Documents and Settings\Admin\Cookies\admin@baidu[2].txt
 Writes to:
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
```

```
Files\Content.IE5\QXMNQBKF\index[1].php
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\CXCXW1MR\baidu_jgylogo3[1].gif
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\QXMNQBKF\jquery-1.10.2.min_f2fb5194[1].js
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\bd_logo1[1].png
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\UH4D6D6X\nuomi_510f7472[1].png
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\CXCXW1MR\icons_0e814c16[1].png
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\zbios_62c636fe[1].png
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\CXCXW1MR\all_async_search_641293e1[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\CXCXW1MR\every_cookie_aa168cb4[1].js
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\3FDD734T\www.baidu[1].xml
                         C:\Documents and Settings\Admin\Cookies\admin@www.baidu[1].txt
 Writes to:
 Writes to:
                         C:\Documents and Settings\Admin\Cookies\admin@www.baidu[2].txt
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\quickdelete_9c14b01a[1].png
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\env_beb83b45[1].swf
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
 Writes to:
Explorer\UserData\index.dat
 Writes to:
                         C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx
 Writes to:
                         C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\macromedia.com\support\flashplayer\sys\settings.sxx
                         C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
 Writes to:
Player\#SharedObjects\45PY3TTW\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
 Writes to:
                         C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\UserData\Z2XJ2MAQ\userDataBIDUPSID[1].xml
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\UH4D6D6X\bdsug_async_dac7ea02[1].js
                         C:\Documents and Settings\Admin\Local
 Writes to:
Settings\History\History.IE5\MSHist012016042220160423\index.dat
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\QXMNQBKF\baiduia_b45d552b[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\JSocket_9a52fc3e[1].swf
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\UH4D6D6X\favicon[1].ico
                         C:\Documents and Settings\Admin\Local
 Writes to:
Settings\Temp\httpwww.baidu.comfavicon.ico
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\nu_instant_search_ebeb5baa[1].js
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\bdbri_icons_2e35e84b[1].png
 Reads from:
                         C:\WINDOWS\Registration\R00000000007.clb
                         C: \verb|\WINDOWS\Temp\1af5338669efabe0a9841478396871b1.exe|\\
 Reads from:
 Reads from:
                         C:\AUTOEXEC.BAT
 Reads from:
                         C:\WINDOWS\system32\drivers\etc\hosts
                         C:\WINDOWS\system32\rsaenh.dll
 Reads from:
                         C:\WINDOWS\win.ini
 Reads from:
 Reads from:
                         C:\WINDOWS\system32\dxtmsft.dll
 Reads from:
                         C:\WINDOWS\system32\dxtrans.dll
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\jquery-1.10.2.min_f2fb5194[1].js
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Reads from:
Files\Content.IE5\CXCXW1MR\every_cookie_aa168cb4[1].js
 Reads from:
                         C:\WINDOWS\system32\Macromed\Flash\mms.cfg
 Reads from:
                         C:\WINDOWS\system32\Macromed\Flash\Flash10h.ocx
 Reads from:
                         C:\WINDOWS\system32\stdole2.tlb
 Reads from:
                         C:\WINDOWS\system32\iepeers.dll
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\all_async_search_641293e1[1].js
                         C:\WINDOWS\system32\mshtml.tlb
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\ONWV4FIP\env_beb83b45[1].swf
                         C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
 Reads from:
Player\macromedia.com\support\flashplayer\sys\settings.sol
                         C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
Player\#SharedObjects\45PY3TTW\s1.bdstatic.com\sharedObjectBIDUPSID.sxx
 Reads from:
                         C:\WINDOWS\system32\ieframe.dll
                         C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\bdsug_async_dac7ea02[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\baiduia_b45d552b[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Application Data\Macromedia\Flash
```

```
Player\macromedia.com\support\flashplayer\sys\settings.sxx
```

C:\Documents and Settings\Admin\Local Settings\Temporary Internet Reads from:

Files\Content.IE5\ONWV4FIP\JSocket_9a52fc3e[1].swf

Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet

Files\Content.IE5\UH4D6D6X\favicon[1].ico

Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet

Files\Content.IE5\QXMNQBKF\nu_instant_search_ebeb5baa[1].js

C:\Documents and Settings\Admin\Cookies\admin@baidu[1].txt Deletes: Deletes: C:\Documents and Settings\Admin\Cookies\admin@baidu[2].txt Deletes: C:\Documents and Settings\Admin\Cookies\admin@www.baidu[1].txt Deletes: ${\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Macromedia\Flash}$

Player\macromedia.com\support\flashplayer\sys\#s1.bdstatic.com\settings.sxx

C:\Documents and Settings\Admin\Application Data\Macromedia\Flash

Player\macromedia.com\support\flashplayer\sys\settings.sol

C:\Documents and Settings\Admin\Application Data\Macromedia\Flash Deletes:

Player\macromedia.com\support\flashplayer\sys\settings.sxx

Deletes: C:\Documents and Settings\Admin\Application Data\Macromedia\Flash

Player\#SharedObjects\45PY3TTW\s1.bdstatic.com\sharedObjectBIDUPSID.sxx

Deletes: C:\Documents and Settings\Admin\Local $Settings \verb|\History\History\IE5\MSHist012014033120140407\verb|\Lindex.dat| \\$ Deletes: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\MSHist012014033120140407

C:\Documents and Settings\Admin\Local Deletes: Settings\History\History.IE5\MSHist012014041220140413\index.dat

C:\Documents and Settings\Admin\Local

Settings\History\History.IE5\MSHist012014041220140413

Network Events

DNS query: www.baidu.com DNS query: s1.bdstatic.com DNS query: sclick.baidu.com DNS guery: formi.baidu.com

www.a.shifen.com ⇒ 103.235.46.39 DNS response: DNS response: wwwstatic1.gshifen.com ⇒ 103.235.44.90 s.a.shifen.com ⇒ 123.125.115.95 DNS response: DNS response: formi.baidu.com ⇒ 61.135.169.120 formi.baidu.com ⇒ 180.149.131.55 DNS response:

127.0.0.1:1039 Connects to: Connects to: 103.235.46.39:80 103.235.44.90:80 Connects to: Connects to: 123,125,115,95:80 Connects to: 61.135.169.120:843 61.135.169.120:8843 Connects to:

Sends data to: 8.8.8.8:53 Sends data to: 127.0.0.1:1039

Sends data to: www.a.shifen.com:80 (103.235.46.39) wwwstatic1.gshifen.com:80 (103.235.44.90) Sends data to: Sends data to: s.a.shifen.com:80 (123.125.115.95)

Receives data from: 0.0.0.0:0 127.0.0.1:1039 Receives data from:

www.a.shifen.com:80 (103.235.46.39) Receives data from: Receives data from: wwwstatic1.gshifen.com:80 (103.235.44.90) Receives data from: s.a.shifen.com:80 (123.125.115.95)

Windows Registry Events

Creates key: HKCU\software\explore

Creates key: $\label{thm:locked} \verb+HKLM\software\microsoft\windows\currentversion\shell extensions\shell extensions \verb+locked+ and the locked+ and the locked of the lock$ HKCU\software\microsoft\windows\currentversion\shell extensions\blocked Creates key: Creates key: HKLM\software\microsoft\windows\currentversion\shell extensions\cached Creates key: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\shell} extensions\cached}$ Creates key: HKCU\software\microsoft\windows\currentversion\internet settings Creates key: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders

Creates key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders

HKLM\software\microsoft\tracing Creates key:

Creates key: HKLM\software\microsoft\windows\currentversion\explorer\user shell

folders

Creates kev: HKCU\software\microsoft\windows nt\currentversion\winlogon

Creates key: HKLM\software\microsoft\windows\currentversion\explorer\shell folders

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

settings\connections

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

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

Creates kev: HKCU\software\microsoft\windows nt\currentversion\network\location

awareness

Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters Creates key: HKCU\software\microsoft\windows\currentversion\internet

settings\p3p\history

HKLM\software\microsoft\directdraw\mostrecentapplication Creates key: Creates key: HKLM\software\microsoft\direct3d\mostrecentapplication Creates key: HKCU\software\microsoft\windows script\settings

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

settings\5.0\cache\extensible cache\userdata HKCU\software\microsoft\internet explorer\domstorage\total Creates key: Creates key: HKCU\software\microsoft\internet explorer\domstorage\baidu.com HKCU\software\macromedia\flashplayer Creates key: Creates kev: 806d6172696f}\ HKCU\software\microsoft\windows\currentversion\internet Creates key: settings\5.0\cache\extensible cache\mshist012016042220160423 Creates key: HKCU\software\microsoft\internet explorer\main\windowssearch HKLM\software\microsoft\downloadmanager Creates kev: Deletes value: $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ settings[proxyserver] Deletes value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyoverride] Deletes value: HKCU\software\microsoft\windows\currentversion\internet settings[autoconfigurl] Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\1af5338669efabe0a9841478396871b1.exe HKLM\system\currentcontrolset\control\terminal server Opens key: Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots HKLM\svstem\currentcontrolset\control\safeboot\option Opens kev: Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\gdi32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\user32.dll Opens key: HKLM\system\currentcontrolset\control\session manager Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\imm32.dll Opens key: $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ options\ntdll.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\secur32.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\rpcrt4.dll Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$ options\advapi32.dll Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\shlwapi.dll Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$ options\shell32.dll Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ole32.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\oleaut32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comctl32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msimg32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\iertutil.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\urlmon.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\version.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\ws2help.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ws2_32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\psapi.dll Opens key: HKLM\system\currentcontrolset\control\error message instrument\ Opens kev: HKLM\svstem\currentcontrolset\control\error message instrument Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32 Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility Opens key: HKLM\software\microsoft\windows nt\currentversion\windows Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ winlogon$ Opens key: HKLM\ Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics Opens key: $\label{lem:hard-wich} \parbox{$HKLM\software\mbox{$\mbox{$\mbox{$w$} indows\currentversion}$} explorer\parbox{$\mbox{$\mbox{$\mbox{$w$} indows}$} \parbox{$\mbox{$ Opens key: HKLM\system\setup

HKCU\software\policies\microsoft\control panel\desktop

Opens key:

Opens key:

Opens key:

Opens key:

HKCU\

HKCU\control panel\desktop

HKLM\software\microsoft\ole

HKCR\interface Opens key: Opens key: HKCR\interface\{00020400-0000-0000-c000-00000000046} Opens kev: HKLM\software\microsoft\oleaut Opens key: HKLM\software\microsoft\oleaut\userera Opens kev: HKCU\software\microsoft\windows\currentversion\explorer\advanced Opens key: $\label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + nt + current + version + language pack$ Opens key: HKCU\software\classes\ HKCU\software\classes\protocols\name-space handler\ Opens key: Opens key: HKCR\protocols\name-space handler HKCU\software\classes\protocols\name-space handler Opens key: Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings Opens key: HKLM\software\microsoft\windows\currentversion\internet settings $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet$ Opens key: settings Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\ Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\ HKCU\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zonemap\domains\ Opens key: settings\zonemap\ranges\ Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}$ settings\zonemap\ranges\ HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_unc_savedfilecheck HKLM\software\microsoft\internet Opens key: $\verb|explorer\main\featurecontrol\feature_unc_savedfilecheck| \\$ Opens key: HKCU\software\microsoft\internet explorer\main Opens kev: options\msctf.dll

HKLM\software\policies\microsoft\windows\currentversion\internet

HKLM\software\microsoft\windows nt\currentversion\image file execution

HKLM\software\microsoft\ctf\compatibility\1af5338669efabe0a9841478396871b1.exe

Opens key:

Opens key: HKCU\keyboard layout\toggle Opens kev: HKLM\software\microsoft\ctf\

HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key:

options\uxtheme.dll

Opens key: HKCU\software\microsoft\windows\currentversion\thememanager Opens key: HKLM\software\microsoft\windows nt\currentversion\imm

Opens key: $\label{local-operator} \mbox{HKCU\software\mbox{\sc microsoft\windows} nt\current version\app compatflags\layers} \\$ Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msctfime.ime

Opens key: HKCU\software\microsoft\ctf

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes

Opens key: HKCU\software\explore

Opens key: HKLM\software\microsoft\com3

 $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ Opens key:

options\comres.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\clbcatq.dll

Opens key: HKLM\software\microsoft\com3\debug

Opens key: HKLM\software\classes

HKU\ Opens key: Opens key: HKCR\clsid

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

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

00c04fd705a2}\treatas

 $\label{locality} $HKCR\clsid_{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas$ Opens key: Opens key:

00c04fd705a2}\inprocserver32

HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32 Opens key:

HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-Opens key:

00c04fd705a2}\inprocserverx86

HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserverx86 Opens key:

Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\localserver32

Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\localserver32 Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\inprochandler32

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

Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\inprochandlerx86

Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\localserver

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\ieframe.dll

Opens key: HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe

Opens key: HKLM\software\microsoft\internet explorer\setup
Opens key: HKLM\system\currentcontrolset\control\wmi\security
Opens key: HKCU\software\classes\interface\{eab22ac1-30c1-11cf-a7eb-

0000c05bae0b}\typelib

Opens key: HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib
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\interface\{b722bccb-4e68-101b-a2bc-

00aa00404770}\proxystubclsid32

Opens key: HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32

Opens key: HKCU\software\classes\interface\{79eac9c4-baf9-11ce-8c82-

00aa004ba90b}\proxystubclsid32

Opens key: HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32

Opens key: HKCU\software\classes\interface\{000214e6-0000-0000-c000-

 ${\tt 000000000046} \verb|\proxystubclsid32| \\$

Opens key: HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32

Opens key: HKCU\software\classes\interface\{93f2f68c-1d1b-11d3-a30e-

00c04f79abd1}\proxystubclsid32

Opens key: HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32

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

Opens key: HKLM\software\microsoft\rpc

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKCU\software\classes\clsid\{889d2feb-5411-4565-8998-1dd2c5261283}

Opens key: HKCR\clsid\{889d2feb-5411-4565-8998-1dd2c5261283}
Opens key: HKCU\software\policies\microsoft\windows\app management
Opens key: HKLM\software\policies\microsoft\windows\app management

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

Opens key: $\label{eq:hkcr} \mbox{HKCR\clsid\coulong} \mbox{ } \mbox{HKCR\clsid\coulong} \mbox{ } \mbox{004b0726-a010-4abf-8556-fcdb7f1fca1e} \mbox{ } \mbo$

Opens key: ${\tt HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus internet \ settings}$

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_http_username_password_disable

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_http_username_password_disable

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562

Opens key: HKCU\software\microsoft\internet

 $explorer \verb|\main| featurecontrol| feature_use_ietldlist_for_domain_determination$

Opens key: HKLM\software\microsoft\internet

Opens key: HKCU\software\policies\microsoft\internet explorer\main
Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer

Opens key: Opens key:

 $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\spaceshape}} \mbox{\tt policies\explorer} \mbox{\tt explorer} \mbox{\tt microsoft\windows\currentversion\spaceshape}} \mbox{\tt policies\explorer} \mbox{\tt explorer} \mbox{\tt$

a2ea-08002b30309d}

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

08002b30309d}\inprocserver32

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\apphelp.dll

 $\label{lem:control} Opens key: $$ HKLM\system\currentcontrolset\control\session manager\appcompatibility Opens key: $$ HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}$$$

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

08002b30309d}\treatas

Opens key: $\label{eq:hccn} \begin{tabular}{ll} HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treat as \\ Opens key: \\ HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treat as \\ \begin{tabular}{ll} HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treat as \\ \begin{tabular}{ll} HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treat as \\ \begin{tabular}{ll} HKCU\software\classes\clsid$

08002b30309d}\inprocserverx86

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserverx86

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

08002b30309d}\localserver32

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver32

HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-Opens key: 08002b30309d}\inprochandler32 Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler32 HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-Opens key: 08002b30309d}\inprochandlerx86 Opens key: $HKCR \ clsid \ \{871c5380-42a0-1069-a2ea-08002b30309d\} \ inprochandler x 86 \ inprochandler$ HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-Opens key: 08002b30309d}\localserver $HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver$ Opens key: Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_iedde_register_protocol Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_iedde_register_protocol Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\normaliz.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wininet.dll Opens key: HKLM\software\policies Opens key: HKCU\software\policies HKCU\software Opens key: Opens key: HKLM\software Opens key: HKLM\software\policies\microsoft\internet explorer Opens kev: HKI M\software\microsoft\windows\currentversion\internet settings\5.0\cache Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\content $\label{lem:hklm} \verb+ HKLM \+ software \+ microsoft \+ windows \+ current version \+ internet$ Opens key: settings\5.0\cache\content HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\cache\cookies HKLM\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\cookies HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\history HKLM\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\cache\history HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\extensible cache HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\extensible cache\domstore HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\cache\extensible cache\feedplat HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\extensible cache\iecompat Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\ietld HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\cache\extensible cache\mshist012014033120140407 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012014041220140413 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\privacie: HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\retry headeronlypost onconnectionreset Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_bufferbreaking_818408 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_bufferbreaking_818408 HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\5.0\cache Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}$ settings\5.0\cache Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289 HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149

Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149 HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled Opens key: HKCU\software\microsoft\internet

```
explorer\main\featurecontrol\feature_allow_long_international_filenames
                     HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens key:
                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
                     HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens key:
                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens key:
                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                     HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
                     HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
                     HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
 Opens key:
                     HKLM\system\currentcontrolset\services\winsock2\parameters
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001
 Opens kev:
Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000004
 Opens kev:
Opens kev:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
 Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010
 Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
 Opens key:
HKLM \ system \ current control set \ services \ win sock 2 \ parameters \ name space \_catalog5 \ catalog\_entries \ 00000000000001
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
 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
                     HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
                     HKLM\software\policies\microsoft\internet explorer\browseremulation
 Opens kev:
 Opens key:
                     HKCU\software\policies\microsoft\internet explorer\browseremulation
 Opens key:
                     HKLM\software\microsoft\internet explorer\mediatypeclass
 Opens key:
                     HKLM\software\microsoft\windows\currentversion\internet
settings\accepted documents
 Opens key:
                     HKLM\software\microsoft\windows\currentversion\policies\ratings
 Opens key:
                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
 Opens key:
                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
 Opens key:
                     HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
```

```
Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
 Opens kev:
                          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\
                          HKLM\software\microsoft\windows\currentversion\internet
 Opens key:
settings\zonemap\domains\
 Opens key:
                          HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\msn.com
 Opens key:
                          HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\msn.com\related
                          HKLM\software\policies\microsoft\internet explorer\security
 Opens kev:
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
 Opens key:
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
 Opens kev:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\
                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
 Opens key:
settings\zones\
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\0
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\1
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\2
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\2
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\3
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\3
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\4
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\4
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature localmachine lockdown
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecon
                         trol\feature localmachine lockdown
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\
 Opens key:
                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
settings\lockdown_zones\
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\0
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\0
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\1
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\1
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\2
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\2
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
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
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\4
```

Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\4 $\label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ Opens key: settings\lockdown_zones\4 HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: options\netapi32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasman.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rtutils.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: options\winmm.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\drivers32 Opens key: HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\tapi32.dll Opens key: HKLM\software\microsoft\windows\currentversion\telephony Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasapi32.dll Opens key: HKLM\software\microsoft\tracing\rasapi32 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\userenv.dll Opens key: HKLM\system\currentcontrolset\control\productoptions Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders Opens key: HKLM\software\policies\microsoft\windows\system Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist $\label{lem:hklm} \verb+Kklm \+ system \+ control \+ session manager \+ environment$ Opens key: Opens key: HKLM\software\microsoft\windows\currentversion Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003 Opens key: HKCU\environment Opens key: HKCU\volatile environment HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\sensapi.dll Opens key: HKCU\software\microsoft\internet explorer HKLM\software\microsoft\internet explorer Opens key: Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_mime_handling HKCU\software\classes\protocols\name-space handler\http\ Opens kev: Opens key: HKCR\protocols\name-space handler\http Opens key: HKCU\software\classes\protocols\name-space handler*\ Opens key: HKCR\protocols\name-space handler* Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_enable_compat_logging Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_enable_compat_logging Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\user agent Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\user agent Opens kev: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent HKLM\software\microsoft\windows\currentversion\internet settings\user Opens key: agent\ua tokens Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\user agent\pre platform HKLM\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\user agent\pre platform $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} in the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu$ Opens key: settings\5.0\user agent\pre platform Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\user agent\post platform Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent\post platform Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent\post platform Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_browser_emulation Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_browser_emulation Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_maxconnectionsperserver HKLM\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_maxconnectionsperserver

explorer\main\featurecontrol\feature_maxconnectionsper1_0server

HKCU\software\microsoft\internet

HKLM\software\microsoft\internet

Opens key:

Opens key:

```
explorer \verb|\main| featurecontrol| feature\_max connection sper1\_0 server
```

Opens key: HKCU\software\microsoft\windows\currentversion\urlmon settings
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\http

filters\rpa

Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\http

filters\rpa

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_include_port_in_spn_kb908209

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\mswsock.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\mlang.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\hnetcfg.dll

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

Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\wshtcpip.dll

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

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\travellog
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\travellog
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\autocomplete
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\autocomplete
Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}

Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062} Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-

00c04fd7d062}\treatas

 Opens key:
 HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\treatas

 Opens key:
 HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535

00c04fd7d062}\inprocserver32

Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32

Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-

00c04fd7d062}\inprocserverx86

Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-

00c04fd7d062}\localserver32

Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\localserver32

 $00c04fd7d062 \} \verb|\inprochandler32| \\$

 $Opens~key: \\ HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\\\ \label{eq:clsid} in prochandler 32$

Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-

00c04fd7d062}\inprochandlerx86

 $Opens~key: \\ HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandlerx 86. \\$

Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-

00c04fd7d062}\localserver

Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\localserver

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\browseui.dll

Opens key: HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}

Opens key: HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}
Opens key: HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-

9fe3c77a297a}\treatas

9fe3c77a297a}\inprocserver32
Opens kev: HKCl

Opens key: HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprocserver32

Opens key: HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-

9fe3c77a297a}\inprocserverx86

Opens key: HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-

9fe3c77a297a}\localserver32

Opens key: HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\localserver32

Opens key: HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-

9fe3c77a297a}\inprochandler32

 $Opens~key: \\ HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\nprochandler 32$

Opens key: HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-

9fe3c77a297a}\inprochandlerx86

Opens key: HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-

9fe3c77a297a}\localserver

Opens key: HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\localserver Opens key: HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}

Opens key: HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062} Opens key: HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-

00c04fd7d062}\treatas

```
HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-
 Opens key:
00c04fd7d062}\inprocserver32
                         HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprocserver32
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprocserverx86
                         HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\tinprocserverx86
 Opens key:
                         HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-
 Opens key:
```

00c04fd7d062}\localserver32

HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\localserver32 Opens key:

HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-Opens key:

00c04fd7d062}\inprochandler32

 $HKCR \ clsid \ \ \{00bb2764-6a77-11d0-a535-00c04fd7d062\} \ \ in prochandler 32$ Opens key:

Opens key: HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-

00c04fd7d062}\inprochandlerx86

 $HKCR \ clsid \ \{00bb2764-6a77-11d0-a535-00c04fd7d062\} \ inprochandler x 86 \ inprochandler$ Opens key:

HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-Opens key:

00c04fd7d062}\localserver

 $\label{localserver} HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\localserver$ Opens key: Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}

Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062} Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\treatas

HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treatas Opens kev: Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\inprocserver32

HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\inprocserverx86

HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserverx86 Opens kev:

Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\localserver32

HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\localserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\inprochandler32

Opens key: $HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\tinprochandler 32$

Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\inprochandlerx86

HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandlerx86 Opens key:

Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\localserver

Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\localserver

Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-

00aa005b4383}\inprocserver32

HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32 Opens key: Opens key: HKLM\software\microsoft\windows\currentversion\explorer\advanced

Opens key: HKLM\system\currentcontrolset\control\securityproviders

Opens key: Opens key: $\label{lem:hklm} \verb+Kklm \+ system \+ control \+ lsa \+ spicache \+ msaps spc.dll$

Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll Opens key: Opens key: HKLM\system\currentcontrolset\control\securityproviders\saslprofiles Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\iphlpapi.dll

Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage Opens kev: HKLM\system\currentcontrolset\services\tcpip\parameters\

Opens key: HKLM\system\currentcontrolset\services\netbt\parameters\interfaces

Opens key: HKLM\system\currentcontrolset\services\netbt\parameters

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msv1_0.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\rasadhlp.dll

Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$

options\dnsapi.dll

Opens key: HKLM\svstem\currentcontrolset\services\dnscache\parameters Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters

Opens key:

c7d49d7cecdc}

Opens key: HKLM\software\policies\microsoft\system\dnsclient

Opens key: $HKLM \verb|\software\m| icrosoft \verb|\cryptography\defaults\provider\m| icrosoft strong$

cryptographic provider

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\rsaenh.dll

Opens key: HKLM\software\policies\microsoft\cryptography

HKLM\software\microsoft\cryptography Opens kev: HKLM\software\microsoft\cryptography\offload Opens key: Opens key: HKCU\software\microsoft\ctf\langbaraddin\ Opens key: HKLM\software\microsoft\ctf\langbaraddin\

Opens kev: HKCU\software\microsoft\internet explorer\ietld\lowmic 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
                                     HKCR\mime\database\content type\text/html; charset=utf-8
  Opens key:
                                     HKCU\software\classes\mime\database\content type\text/html
  Opens kev:
  Opens key:
                                     HKCR\mime\database\content type\text/html
  Opens kev:
                                     HKCU\software\classes\protocols\filter\text/html; charset=utf-8
  Opens key:
                                     HKCR\protocols\filter\text/html; charset=utf-8
                                     HKCU\software\classes\protocols\filter\text/html
  Opens key:
                                     HKCR\protocols\filter\text/html
  Opens key:
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing
  Opens kev:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_feeds
                                     HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_feeds
                                     HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_safe_bindtoobject
  Opens key:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject
                                     HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
  Opens key:
                                     HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
  Opens key:
                                     HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
  Opens kev:
00aa00686f13}\treatas
  Opens key:
                                     HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas
                                     HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
  Opens key:
00aa00686f13}\inprocserver32
                                     HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32
  Opens key:
  Opens kev:
                                     HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserverx86
  Opens key:
                                     HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserverx86
  Opens key:
                                     HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\localserver32
  Opens key:
                                     HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\localserver32
                                     HKCU \setminus software \setminus classes \setminus clsid \setminus \{25336920-03f9-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11cf-8fd0-11c
  Opens key:
00aa00686f13}\inprochandler32
  Opens key:
                                     HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler32
  Opens key:
                                     HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprochandlerx86
  Opens key:
                                     HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandlerx86
                                     HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
  Opens key:
00aa00686f13}\localserver
  Opens key:
                                     HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\localserver
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\msls31.dll
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\mshtml.dll
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
                                     HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
                                     HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
                                     HKLM\software\microsoft\internet
  Opens key:
explorer \verb|\main| featurecontrol| feature\_external\_style\_sheet\_fix\_for\_smartnavigation\_kb926131
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_aria_support
  Opens key:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_aria_support
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams
  Opens key:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams
                                     HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_private_font_setting
  Opens key:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_private_font_setting
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_css_show_hide_events
  Opens key:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_css_show_hide_events
                                     HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature display node advise kb833311
  Opens key:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_expanduri_bypass
                                     HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature allow expanduri bypass
  Opens key:
                                     HKCU\software\microsoft\internet
```

 $explorer \verb|\main| featurecontrol| feature_body_size_in_editable_iframe_kb943245$

Opens key:

explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245

HKLM\software\microsoft\internet

```
HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_databinding_support
  Opens kev:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
  Opens kev:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_enforce_bstr
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
                                    HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
                                    HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
  Opens kev:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
  Opens key:
                                    HKCU\software\microsoft\windows nt\currentversion\windows
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fls
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fls
  Opens key:
                                    HKLM\software\microsoft\windows\currentversion\app paths\outlook.exe
  Opens key:
                                    HKLM\software\microsoft\internet explorer\application compatibility
                                    HKLM\software\policies\microsoft\internet explorer\domstorage
  Opens key:
  Opens key:
                                    HKCU\software\policies\microsoft\internet explorer\domstorage
  Opens key:
                                    HKCU\software\microsoft\internet explorer\domstorage
                                    HKLM\software\microsoft\internet explorer\domstorage
  Opens key:
  Opens key:
                                    HKLM\software\policies\microsoft\internet explorer\safety\privacie
  Opens key:
                                    HKCU\software\policies\microsoft\internet explorer\safety\privacie
                                    HKCU\software\microsoft\internet explorer\safety\privacie
  Opens key:
  Opens key:
                                    HKLM\software\microsoft\internet explorer\safety\privacie
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_manage_script_circular_refs
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_manage_script_circular_refs
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_restrict_filedownload
  Opens key:
                                    HKLM\software\microsoft\internet explorer\security\floppy access
                                    HKCU\software\microsoft\internet explorer\security\adv addrbar spoof
  Opens kev:
detection
  Opens key:
                                    HKLM\software\microsoft\internet explorer\security\adv addrbar spoof
detection
  Opens key:
                                    HKCU\software\classes\protocols\name-space handler\about\
                                    HKCR\protocols\name-space handler\about
  Opens key:
  Opens kev:
                                    HKCU\software\classes\protocols\handler\about
  Opens key:
                                    HKCR\protocols\handler\about
  Opens key:
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
                                    HKCU \setminus software \setminus classes \setminus clsid \setminus \{3050f406-98b5-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11c
  Opens key:
00aa00bdce0b}\treatas
  Opens key:
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas
  Opens key:
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
  Opens key:
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
  Opens key:
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserverx86
  Opens key:
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
  Opens key:
00aa00bdce0b}\localserver32
  Opens key:
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver32
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
  Opens key:
00aa00bdce0b}\inprochandler32
  Opens key:
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
  Opens key:
00aa00bdce0b}\inprochandlerx86
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86
  Opens kev:
  Opens key:
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\localserver
  Opens key:
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_document_compatible_mode
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_document_compatible_mode
```

HKLM\software\microsoft\windows\currentversion\internet settings\zones\3 Opens key:

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

Opens key: HKCU\software\microsoft\internet explorer\zoom Opens kev: HKLM\software\microsoft\internet explorer\zoom

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

HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-Opens key:

00aa00686f13}\progid

HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid Opens key:

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

history

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

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

Opens key: HKCU\software\microsoft\internet explorer\international\scripts Opens key: HKLM\software\microsoft\internet explorer\international\scripts Opens key: HKLM\software\policies\microsoft\internet explorer\settings

Opens key: HKCU\software\microsoft\internet explorer\settings Opens key: HKLM\software\microsoft\internet explorer\settings HKCU\software\microsoft\internet explorer\styles Opens key:

HKCU\software\microsoft\windows\currentversion\policies\activedesktop Opens kev:

Opens key: HKCU\software\microsoft\windows\currentversion\policies Opens key: HKCU\software\microsoft\internet explorer\pagesetup HKCU\software\microsoft\internet explorer\menuext Opens key: Opens key: HKCU\software\microsoft\internet explorer\menuext\%s Opens key: HKLM\system\currentcontrolset\control\nls\codepage

HKCU\software\microsoft\internet explorer\international\scripts\3 Opens key:

Opens key: HKLM\software\microsoft\internet explorer\version vector

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

explorer\main\featurecontrol\feature_xssfilter

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_xssfilter

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

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

Opens key: $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ internet\ explorer\+ dxtrans$ Opens key: HKLM\software\microsoft\internet explorer\dxtrans

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_behaviors

HKLM\software\microsoft\internet Opens kev:

explorer\main\featurecontrol\feature_behaviors

Opens key: $\label{lem:hklm} \mbox{\tt HKLM} \mbox{\tt software} \mbox{\tt microsoft} \mbox{\tt internet explorer} \mbox{\tt default behaviors}$ Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{3050f4cf-98b5-11cf-bb82-00aa00bdce0b\}$

Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b} HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-Opens key:

00aa00bdce0b}\treatas

HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\treatas Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-Opens key:

00aa00bdce0b}\inprocserver32

Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32

HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-Opens key:

00aa00bdce0b}\inprocserverx86

Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86

HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-Opens key:

00aa00bdce0b}\localserver32 Opens key:

HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\localserver32

Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-

00aa00bdce0b}\inprochandler32

Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32

Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-

00aa00bdce0b}\inprochandlerx86

Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-

00aa00bdce0b}\localserver

Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\localserver

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\winspool.drv

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\iepeers.dll

Opens key: HKCU\software\policies\microsoft\internet explorer\persistence HKLM\software\policies\microsoft\internet explorer\persistence Opens kev:

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_binary_caller_service_provider

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_binary_caller_service_provider

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_subdownload_lockdown Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_subdownload_lockdown HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_sslux HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_sslux Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}$ settings\ Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\ Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\ Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ Opens key: $\label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\internet}}$ settings\zonemap\ HKLM\software\policies\microsoft\internet explorer\restrictions Opens key: Opens key: HKCU\software\policies\microsoft\internet explorer\restrictions HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc} Opens key: Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc} Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989f4ceaaf59cfc}\treatas Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\treatas Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{50d5107a - d278 - 4871 - 8989 - d278 - d$ f4ceaaf59cfc}\inprocserver32 HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32 Opens kev: Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989f4ceaaf59cfc}\inprocserverx86 HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserverx86 Opens key: Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989f4ceaaf59cfc}\localserver32 HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\localserver32 Opens kev: Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989f4ceaaf59cfc}\inprochandler32 HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandler32 Opens key: Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989f4ceaaf59cfc}\inprochandlerx86 Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandlerx86 Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989f4ceaaf59cfc}\localserver HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\localserver Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msimtf.dll HKLM\software\microsoft\ctf\tip Opens key: Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8c9633f71be64}\languageprofile HKCU\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-Opens key: c9633f71be64}\languageprofile HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-Opens key: $c9633f71be64\\ \\ language profile \\ \\ 0x00000000$ Opens key: $HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8$ c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d} $HKCU \setminus software \setminus classes \setminus clsid \setminus \{3ce74de4-53d3-4d74-8b83-431b3828ba53\}$ Opens key: Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53} Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\treatas HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\treatas Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-Opens kev: 431b3828ba53}\inprocserver32 HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32 Opens key: Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserverx86 Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserverx86 Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver32 HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver32 Opens key: Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandler32 Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandler32 Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandlerx86 Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandlerx86 HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-Opens kev: 431b3828ba53}\localserver Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7} HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7} Opens key: Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\treatas

 431b3828ba53}\inprochandlerx86

 Opens key:
 HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandlerx86

 Opens key:
 HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver

 Opens key:
 HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver

 Opens key:
 HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\

 Opens key:
 HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\

 Opens key:
 HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\treatas

 Opens key:
 HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\treatas

 Opens key:
 HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\tinprocserver32

 Opens key:
 HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\tinprocserver32

 Opens key:
 HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\tinprocserver32

 Opens key:
 HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\tinprocserverx86

 Opens key:
 HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\tinprocserverx86

 Opens key:
 HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\tinprocserverx86

```
Opens key:
                                                                                                                               HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\localserver32
        Opens key:
                                                                                                                               HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\localserver32
                                                                                                                               HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
        Opens key:
869523e2d6c7}\inprochandler32
        Opens key:
                                                                                                                               HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
        Opens key:
869523e2d6c7}\inprochandlerx86
        Opens key:
                                                                                                                               HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandlerx86
                                                                                                                               HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
        Opens key:
869523e2d6c7}\localserver
        Opens key:
                                                                                                                               HKCR \ clsid \ a4b544a1-438d-4b41-9325-869523e2d6c7 \ \ local server
        Opens key:
                                                                                                                               HKLM\software\microsoft\ctf\tip\
                                                                                                                               HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
        Opens key:
c9633f71be64}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
                                                                                                                               HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
        Opens key:
77e8f3d1aa80}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
        Opens key:
                                                                                                                               HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
e988c088ec82}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
                                                                                                                               HKLM \setminus software \setminus microsoft \setminus tip \setminus \{dcbd6fa8-032f-11d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d3-b5b1-14d
        Opens key:
00c04fc324a1}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
                                                                                                                               HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9a
        Opens key:
0 f816 c09 f4 ee \} \\ \\ category \\ \\ category \\ \\ \{b95 f181 b-ea4 c-4 af1-805 6-7 c321 abb b091\} \\ \\
                                                                                                                               HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
        Opens key:
c9633f71be64}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
                                                                                                                               HKLM \setminus software \setminus irrosoft \setminus tip \setminus \{78cb5b0e-26ed-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc
        Opens key:
77e8f3d1aa80}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
                                                                                                                               HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
        Opens key:
e988c088ec82}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
                                                                                                                               HKLM \setminus software \setminus microsoft \setminus tip \setminus \{dcbd6fa8-032f-11d3-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143
        Opens key:
00c04fc324a1}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
                                                                                                                               HKLM \setminus software \setminus irrosoft \setminus tip \setminus \{f89e9e58-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f
        Opens key:
0 f816 c09 f4 ee \} \\ category \\ \{534 c48 c1 - 0607 - 4098 - a521 - 4fc899 c73 e90\} \\ (409 c73 e90) \\ (409 c7
        Opens key:
                                                                                                                               HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
\verb|c9633f71be64| \land \verb|category| item| \{5130a009-5540-4fcf-97eb-aad33fc0ee09\}| \\
                                                                                                                               Opens key:
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
                                                                                                                               HKLM \setminus software \setminus irrosoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 80
        Opens key:
c9633f71be64}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
                                                                                                                               HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
        Opens key:
77e8f3d1aa80\} \\ category \\ item \\ \{7ae86bb7-262c-431e-9111-c974b6b7cac3\} \\
                                                                                                                               HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
        Opens key:
c9633f71be64\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
                                                                                                                               HKLM \setminus software \setminus irrosoft \setminus tip \setminus \{78cb5b0e-26ed-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc
        Opens key:
77e8f3d1aa80\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
        Opens key:
                                                                                                                               HKCU\software\policies\microsoft\internet explorer\control panel
        Opens key:
                                                                                                                              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
       Opens kev:
                                                                                                                              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
                                                                                                                               HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
        Opens kev:
                                                                                                                               HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
        Opens key:
        Opens key:
                                                                                                                               HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\treatas
        Opens kev:
                                                                                                                               HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\treatas
        Opens key:
                                                                                                                               HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32
        Opens key:
                                                                                                                               HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32
                                                                                                                               HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
        Opens key:
00aa00bbbb58}\inprocserverx86
        Opens key:
                                                                                                                               HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserverx86
        Opens key:
                                                                                                                               HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\localserver32
                                                                                                                               HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\localserver32
        Opens kev:
                                                                                                                               HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
        Opens key:
00aa00bbbb58}\inprochandler32
        Opens key:
                                                                                                                               HKCR\clsid\f414c260-6ac0-11cf-b6d1-00aa00bbbb58\\\inprochandler32
                                                                                                                               Opens key:
00aa00bbbb58}\inprochandlerx86
                                                                                                                               HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprochandlerx86
        Opens kev:
        Opens key:
                                                                                                                               HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\localserver
        Opens key:
                                                                                                                               HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\localserver
        Opens key:
                                                                                                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\jscript.dll
        Opens key:
                                                                                                                               HKLM\software\microsoft\windows script\features
        Opens key:
                                                                                                                               HKLM\system\currentcontrolset\control\nls\locale
                                                                                                                               HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
        Opens key:
        Opens key:
                                                                                                                               HKLM\system\currentcontrolset\control\nls\language groups
        Opens key:
                                                                                                                               HKCU\software\classes\appid\1af5338669efabe0a9841478396871b1.exe
        Opens key:
                                                                                                                               HKCR\appid\1af5338669efabe0a9841478396871b1.exe
        Opens key:
                                                                                                                               HKLM\svstem\currentcontrolset\control\lsa
```

HKLM\software\policies\microsoft\internet explorer\recovery

Opens key:

Opens key: HKCU\software\microsoft\internet explorer\recovery Opens key: HKLM\software\microsoft\internet explorer\recovery

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_scripturl_mitigation Opens kev: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_scripturl_mitigation Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_block_lmz_img Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_block_lmz_img

Opens key: HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}

Opens key: $HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd\}$ Opens key: HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-

dc030521aabd}\treatas

Opens key: $HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\treatas$ HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-Opens key:

dc030521aabd}\inprocserver32

Opens key: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32

Opens key: HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-

dc030521aabd}\inprocserverx86

Opens key: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-

dc030521aabd}\localserver32

Opens key: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\localserver32

Opens key: HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-

dc030521aabd}\inprochandler32

Opens key: $HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprochandler 32$

Opens key: HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-

dc030521aabd}\inprochandlerx86

Opens key: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-

dc030521aabd}\localserver

Opens key: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\localserver

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\atl.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\dxtrans.dll

HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key:

options\xpsp2res.dll

HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000} Opens key:

HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000} Opens key: Opens key: HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-

3c8b00c10000}\treatas

HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\treatas Opens key: HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-Opens kev:

3c8b00c10000}\inprocserver32

 $HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\\\\inprocserver32$ Opens key: Opens key:

HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserverx86

 $\label{lem:hkcr} $$ HKCR\clsid\\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\\{inprocserverx86} $$$ Opens key: HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-Opens kev:

3c8b00c10000}\localserver32

Opens key:

 $HKCR \ clsid \ \{d1fe6762-fc48-11d0-883a-3c8b00c10000\} \ localserver 32$

 $HKCU \setminus software \setminus classes \setminus clsid \setminus \{d1fe6762 - fc48 - 11d0 - 883a - fc48 - f$ Opens key:

3c8b00c10000}\inprochandler32

Opens key: $\label{localization} $HKCR\clsid_{d1fe6762-fc48-11d0-883a-3c8b00c10000}\nprochandler 32 $$$

HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-Opens key:

3c8b00c10000}\inprochandlerx86

HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprochandlerx86 Opens key:

Opens key: HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-

3c8b00c10000}\localserver

HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\localserver Opens key: Opens key: HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}

Opens key: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d} Opens key: HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-

00c04fd9189d}\treatas

Opens key: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\treatas HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-Opens key:

00c04fd9189d}\inprocserver32

HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32 Opens kev:

Opens key: HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-

00c04fd9189d}\inprocserverx86

Opens key: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserverx86

HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-Opens key:

00c04fd9189d}\localserver32

HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\localserver32 Opens kev:

Opens key: HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-

00c04fd9189d}\inprochandler32

Opens key: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprochandler32

Opens key: HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-

00c04fd9189d}\inprochandlerx86

HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprochandlerx86 Opens kev:

Opens key: HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-

```
HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\localserver
 Opens kev:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\dciman32.dll
 Opens kev:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ddraw.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ddrawex.dll
 Opens key:
                         HKLM\hardware\devicemap\video
 Opens key:
                         HKLM\software\microsoft\directdraw\compatibility
                         HKLM\software\microsoft\directdraw\compatibility\bug!
 Opens key:
                         HKLM\software\microsoft\directdraw\compatibility\demolitionderby2
 Opens key:
 Opens key:
                         HKLM\software\microsoft\directdraw\compatibility\mortalkombat3
                         HKLM\software\microsoft\directdraw\compatibility\msgolf98
 Opens key:
                         HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay
 Opens key:
                         HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo
 Opens key:
                         HKLM\software\microsoft\directdraw\compatibility\rogue squadron
 Opens kev:
 Opens key:
                         HKLM\software\microsoft\directdraw\compatibility\savage
 Opens key:
                         HKLM\software\microsoft\directdraw\compatibility\scorchedplanet
 Opens key:
                         HKLM\software\microsoft\directdraw\compatibility\silentthunder
 Opens key:
                         HKLM\software\microsoft\directdraw\compatibility\terracide
 Opens key:
                         HKLM\software\microsoft\directdraw\compatibility\thirddimension
 Opens kev:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark
 Opens key:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark
 Opens key:
                         HKLM\software\microsoft\directdraw\gammacalibrator
 Opens key:
                         HKLM\software\microsoft\directdraw
 Opens key:
                         HKLM\software\microsoft\direct3d
 Opens key:
                         HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}
 Opens key:
                         HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}
 Opens key:
                         HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\treatas
 Opens key:
                         HKCR\clsid{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\treatas
                         HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
 Opens key:
f941e9b7e1fe}\inprocserver32
 Opens key:
                         HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32
                         HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
 Opens key:
f941e9b7e1fe}\inprocserverx86
                         HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserverx86
 Opens key:
                         HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
 Opens key:
f941e9b7e1fe}\localserver32
 Opens key:
                         HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\localserver32
                         HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
 Opens key:
f941e9b7e1fe}\inprochandler32
 Opens key:
                         HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprochandler32
                         HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
 Opens key:
f941e9b7e1fe}\inprochandlerx86
                         HKCR\clsid{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprochandlerx86
 Opens kev:
                         HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
 Opens key:
f941e9b7e1fe}\localserver
 Opens key:
                         HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\localserver
 Opens key:
                         HKCU\software\classes\dximagetransform.microsoft.shadow
 Opens key:
                         HKCR\dximagetransform.microsoft.shadow
 Opens kev:
                         HKCU\software\classes\dximagetransform.microsoft.shadow\clsid
 Opens key:
                         HKCR\dximagetransform.microsoft.shadow\clsid
 Opens key:
                         HKCU \setminus software \setminus classes \setminus clsid \setminus \{e71b4063-3e59-11d2-952a-00c04fa34f05\}
 Opens key:
                         HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}
 Opens key:
                         HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\treatas
 Opens key:
                         HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\treatas
 Opens key:
                         \label{lem:hklm} \verb+Kklm \+ software + microsoft + internet explorer + activex compatibility
 Opens key:
                         HKLM\software\microsoft\internet explorer\activex
compatibility\{e71b4063-3e59-11d2-952a-00c04fa34f05}
                         HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-
 Opens key:
00c04fa34f05}\inprocserver32
 Opens key:
                         HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprocserver32
                         Opens key:
00c04fa34f05}\inprocserverx86
 Opens key:
                         HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\inprocserverx86
                         HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-
 Opens key:
00c04fa34f05}\localserver32
 Opens key:
                         HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\localserver32
 Opens key:
                         HKCU\software\classes\mime\database\content type\image/gif
 Opens key:
                         HKCR\mime\database\content type\image/gif
                         HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-
 Opens key:
00c04fa34f05}\inprochandler32
                         Opens kev:
                         HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-
 Opens key:
00c04fa34f05}\inprochandlerx86
 Opens key:
                         HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\\\\
                         HKCU\software\classes\clsid\{e71b4063-3e59-11d2-952a-
 Opens key:
00c04fa34f05}\localserver
```

00c04fd9189d}\localserver

Opens key: HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\localserver

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\dxtmsft.dll

Opens key: HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}

 Opens key:
 HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db\}

 Opens key:
 HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e

0000f87557db}\treatas

Opens key: HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\treatas Opens key: HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-

0000f87557db}\inprocserver32

Opens key: HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32

Opens key: HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-

0000f87557db}\inprocserverx86

Opens key: HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-

0000f87557db}\localserver32

Opens key: HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\localserver32

Opens key: HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-

0000f87557db}\inprochandler32

Opens key: HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprochandler32

Opens key: HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-

0000f87557db}\inprochandlerx86

Opens key: HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-

0000f87557db}\localserver

Opens key: $\label{eq:hkcnlsid} \begin{tabular}{ll} HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\localserver \\ Opens key: \\ HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd} \end{tabular}$

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

f4fc1e6ca1bd}\treatas

Opens key: $\label{eq:hccn} \begin{tabular}{ll} HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\treatas \\ Opens key: \\ HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-} \\ \end{tabular}$

f4fc1e6ca1bd}\inprocserver32

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

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

f4fc1e6ca1bd}\inprocserverx86

Opens key: HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserverx86

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

f4fc1e6ca1bd}\localserver32

Opens key: HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\localserver32

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

f4fc1e6ca1bd}\inprochandler32

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

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

f4fc1e6ca1bd}\inprochandlerx86

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

f4fc1e6ca1bd}\localserver

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\sxs.dll

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

 $\label{lem:continuous} Opens \ key: \\ Opens \ key: \\ HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\label{lem:continuous} +1.1\409$

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

00aa003b6061}\1.1\0\win32

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

 $\label{lem:continuous} 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 kev: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_disable_behaviors_draw_reentrancy

Opens kev: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_disable_behaviors_draw_reentrancy

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

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

00aa003f8646}\treatas

00aa003f8646}\inprocserver32

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

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

00aa003f8646}\inprocserverx86

Opens key: HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserverx86

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

00aa003f8646}\localserver32

Opens key: HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\localserver32

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

00aa003f8646}\inprochandler32

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

00aa003f8646}\inprochandlerx86

Opens key: HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprochandlerx86

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

00aa003f8646}\localserver

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

Opens key: HKCU\software\classes\mime\database\content type\application/javascript

Opens key: HKCR\mime\database\content type\application/javascript

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561

Opens key: HKCU\software\classes\mime\database\content type\image/png

Opens key: HKCR\mime\database\content type\image/png

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\imgutil.dll

Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}

Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}
Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-

00aa006c1a01}\treatas

 $\label{lem:openskey:openskey: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01\}\treatas} \\ Openskey: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01\}\treatas} \\ Openskey: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01\}\treatas} \\ Openskey: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01\}\treatas} \\ Openskey: HKCU\software\classes\clsid\cl\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsi$

00aa006c1a01}\inprocserver32

Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32

Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-

00aa006c1a01}\inprocserverx86

Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserverx86

Opens key: $\label{localized hkcusoftware classes clsid and a constraint of the con$

00aa006c1a01}\localserver32

Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver32
Opens key: HKCU\software\microsoft\internet explorer\international\scripts\24

Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-

00aa006c1a01}\inprochandler32

Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandler32

Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-

00aa006c1a01}\inprochandlerx86

Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-

00aa006c1a01}\localserver

Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver
Opens key: HKCU\software\microsoft\internet explorer\international\scripts\26
Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}

 $\label{lem:continuous} Opens key: $$ HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01\}$} Opens key: $$ HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01\}$}$

00aa006c1a01}\treatas

00aa006c1a01}\inprocserver32

 $Opens~key: \\ HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32$

Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-

00aa006c1a01}\inprocserverx86

Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-

00aa006c1a01}\localserver32

Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver32

Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-

00aa006c1a01}\inprochandler32

Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandler32

Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-

00aa006c1a01}\inprochandlerx86

```
HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01\}\ \ inprochandlerx86
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\localserver
                         HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver
 Opens key:
 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
                         HKCR\mime\database\content type\image/bmp\bits
 Opens key:
 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:
                         {\tt HKCR\mbox{\tt Mime}\database\content\ type\limage/jpeg\bits}
 Opens key:
                         HKCU\software\classes\mime\database\content type\image/pjpeg\bits
 Opens key:
                         HKCR\mime\database\content type\image/pjpeg\bits
 Opens key:
                         HKCU\software\classes\mime\database\content type\image/png\bits
 Opens key:
                         HKCR\mime\database\content type\image/png\bits
 Opens kev:
                         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 kev:
                         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\mbox{\tt Mime}\database\content\ type\limage/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
                         HKCU \setminus software \setminus classes \setminus clsid \setminus \{a3ccedf7-2de2-11d0-86f4-00a0c913f750\}
 Opens key:
 Opens key:
                         HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}
 Opens key:
                         HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\treatas
 Opens key:
                         HKCR\clsid\a3ccedf7-2de2-11d0-86f4-00a0c913f750\treatas
 Opens key:
                         HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32
                         HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
 Opens kev:
00a0c913f750}\inprocserverx86
                         HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\\\\
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\localserver32
                         HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver32
 Opens key:
                         HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
 Opens kev:
00a0c913f750}\inprochandler32
                         HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandler32
 Opens kev:
                         HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
 Opens key:
00a0c913f750}\inprochandlerx86
 Opens key:
                         HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandlerx86
                         HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
 Opens kev:
00a0c913f750}\localserver
                         HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver
 Opens key:
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\pngfilt.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdiplus.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\d3dim700.dll
                         HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
 Opens key:
c9633f71be64}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                         HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
 Opens key:
77e8f3d1aa80}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                         Opens key:
e988c088ec82}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                         HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
 Opens kev:
00c04fc324a1}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                         HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-
 Opens kev:
Of816cO9f4ee}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
 Opens key:
                         HKCU\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature\_cross\_domain\_redirect\_mitigation| \\
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation
 Opens kev:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature block lmz script
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_script
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_windowedselectcontrol
```

HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_use_windowedselectcontrol

Opens key:

Opens key: HKCU\software\microsoft\internet explorer\new windows
Opens key: HKLM\software\microsoft\internet explorer\new windows

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_xmlhttp

Opens key: HKLM\software\microsoft\internet

 $\verb|explorer\main\featurecontrol\feature_xmlhttp|\\$

Opens key: HKCU\software\classes\shockwaveflash.shockwaveflash

Opens key: HKCR\shockwaveflash.shockwaveflash

Opens key: HKCU\software\classes\shockwaveflash.shockwaveflash\clsid

Opens key: HKCR\shockwaveflash.shockwaveflash\clsid

Opens key: HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}

Opens key: HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}
Opens key: HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-

444553540000}\treatas

444553540000}\inprocserver32

Opens key: HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprocserver32

Opens key: HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-

444553540000}\inprocserverx86

Opens key: HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-

444553540000}\localserver32

Opens key: HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\localserver32

Opens key: HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-

444553540000}\inprochandler32

Opens key: HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprochandler32

Opens key: HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-

444553540000}\inprochandlerx86

Opens key: HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-

444553540000}\localserver

Opens key: HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\localserver

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msasn1.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\crypt32.dll

Opens key: HKLM\system\currentcontrolset\services\crypt32\performance
Opens key: HKLM\software\microsoft\windows nt\currentversion\msasn1

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\dsound.dll

Opens key: HKLM\software\microsoft\directx

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\comdlg32.dll

Opens key: ${\tt HKLM \setminus software \setminus microsoft \setminus windows\ nt \setminus current version \setminus image\ file\ execution}$

options\mscms.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\flash10h.ocx

Opens key: HKLM\hardware\description\system\centralprocessor\0

Opens key: HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}

Opens key: $\label{eq:hkcr} \mbox{HKCR\typelib} \ \{\mbox{d27cdb6b-ae6d-11cf-96b8-444553540000}\}$

444553540000}\1.0\409

444553540000}\1.0\9

 $\label{lem:continuous} Opens~key: $$ HKCR\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000\}\1.0\9 $$ Opens~key: $$ HKCU\software\classes\typelib\{d27cdb6b-ae6d-11cf-96b8-444553540000}\$

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-96b8-44455354000}\1.0\0\win32 Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-c000-00000000046}

Opens key: HKCR\typelib\{00020430-0000-0000-0000-00000000046}

Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-0000-00000000046}\2.0

000000000046}\2.0\0 Opens key:

000000000046}\2.0\0\win32

Opens key: HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}

Opens key: HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0

Opens key: $\label{eq:hkcntypelib} $$ HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0$ Opens key: <math display="block">\label{eq:hkcutypelib} $$ HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\$

00c04fb6bfc4}\1.0\0

Opens key: $\label{eq:hkcr} \begin{tabular}{ll} HKCR\typelib\f-e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\label{eq:hkcr} 1.0\label{eq:hkcr} Opens key: <math display="block">\begin{tabular}{ll} HKCU\software\classes\typelib\f-e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\label{eq:hkcr} \end{tabular}$

```
00c04fb6bfc4}\1.0\0\win32
```

Opens key: HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32

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

explorer\main\featurecontrol\feature_domstorage

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\xmllite.dll

Opens key:

HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{20d04fe0-3aea-1069-

a2d8-08002b30309d}

Opens key: HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\inprocserver32

Opens key: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32

Opens key: HKCU\software\classes\drive\shellex\folderextensions

Opens key: HKCR\drive\shellex\folderextensions

Opens key: HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-

4442-804e-409d6c4515e9}

Opens key: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-

409d6c4515e9}

Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}

Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4\}
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\treatas

Opens key: $\begin{tabular}{ll} HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas \\ Opens key: \\ HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-} \\ \end{tabular}$

00c04fb6bfc4}\inprocserver32

Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32

Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\inprocserverx86

Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\localserver32

Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver32

Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\inprochandler32

Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32

Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\inprochandlerx86

Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\localserver

Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver Opens key: HKCU\software\microsoft\internet explorer\feed discovery Opens key: HKLM\software\microsoft\internet explorer\feed discovery

Opens key: HKCU\software\microsoft\ftp

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

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

compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}

Opens key: HKCU\software\classes\clsid\{aaf8c6ce-f972-11d0-97eb-00aa00615333}

Opens key: HKCR\clsid\{aaf8c6ce-f972-11d0-97eb-00aa00615333}

Opens key: HKCU\software\microsoft\code store database\distribution units
Opens key: HKLM\software\microsoft\code store database\distribution units
Opens key: HKLM\software\microsoft\code store database\distribution

units\{d27cdb6e-ae6d-11cf-96b8-444553540000}

Opens key: HKCU\software\classes\clsid

Opens key: HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-

444553540000}\availableversion

Opens key: HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\availableversion

Opens key: HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-

444553540000}\installedversion

Opens key: $HKCR\clsid\d27cdb6e-ae6d-11cf-96b8-444553540000\nstalledversion$ Opens key: $HKCU\software\classes\clsid\d27cdb6e-ae6d-11cf-96b8-444553540000\arrowversion$

Opens key: $\begin{tabular}{ll} HKCR\clsid\d27cdb6e-ae6d-11cf-96b8-444553540000\appid \\ Opens key: \\ HKCU\software\classes\clsid\d27cdb6e-ae6d-11cf-96b8- \\ \end{tabular}$

444553540000}\languagecheckperiod

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_consult_mime_killbit_kb905915

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_consult_mime_killbit_kb905915

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

explorer\main\featurecontrol\feature_activex_repurposedetection

Opens key: HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-

444553540000}\miscstatus

Opens key: $\label{eq:hkcr} \mbox{HKCR\clsid\d27cdb6e-ae6d-11cf-96b8-444553540000} \mbox{\mbox{$\mbox{\mb

Opens key: HKCU\software\classes\clsid\{d27cdb6e-ae6d-11cf-96b8-

444553540000}\miscstatus\1

Opens key: HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\miscstatus\1
Opens key: HKCU\software\classes\mime\database\content type\application/x-

shockwave-flash

 $\label{lem:content_type_application/x-shockwave-flash} Opens key: $$ HKCU\software\classes\protocols\filter\application/x-shockwave-flash $$$

Opens key: HKCR\protocols\filter\application/x-shockwave-flash

Opens key: HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}

Opens key: HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}
Opens key: HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-

00c04f983e60}\treatas

Opens key: $\begin{tabular}{ll} HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\treatas \\ Opens key: \\ HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-11d2-b$

00c04f983e60}\inprocserver32

Opens key: HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprocserver32

Opens key: $\label{local-condition} \begin{tabular}{ll} HKCU\software\microsoft\multimedia\sound\mbox{ mapper} \\ Opens key: \\ HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-1} \\ \end{tabular}$

00c04f983e60}\inprocserverx86

Opens key: HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-

00c04f983e60}\localserver32

Opens key: HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-

00c04f983e60}\inprochandler32

Opens key: HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprochandler32

Opens key: HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-

00c04f983e60}\inprochandlerx86

Opens key: HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{2933bf90-7b36-11d2-b20e-

00c04f983e60}\localserver

Opens key: HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\localserver

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msxml3.dll

Opens key: HKLM\software\microsoft\msxml30

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

settings\5.0\cache\extensible cache\userdata

Opens key: HKCU\software\microsoft\cryptography\providers\type 001

Opens key: HKLM\software\microsoft\cryptography\defaults\provider types\type 001
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\schannel.dll

Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}

00a0c90a8f39}\treatas

00a0c90a8f39}\inprocserver32

Opens key: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserver32

Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-

00a0c90a8f39}\inprocserverx86

Opens key: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-

00a0c90a8f39}\localserver32

Opens key: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\localserver32

Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-

00a0c90a8f39}\inprochandler32

 $Opens~key: \\ HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\\\ \ inprochandler 32$

Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-

00a0c90a8f39}\inprochandlerx86

Opens key: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-

00a0c90a8f39}\localserver

 $Opens~key: \\ HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\localserver$

 $Opens~key: \\ HKCU \setminus software \setminus \{85cb6900-4d95-11cf-960c-0080c7f4ee85\}$

 Opens key:
 HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}

 Opens key:
 HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}

0080c7f4ee85}\proxystubclsid32

 Opens key:
 HKCR\clsid\{00020424-0000-0000-c000-000000000046\}

 Opens key:
 HKCU\software\classes\clsid\{00020424-0000-0000-c000-c000-c000-c0000-c0000-c0000-c000-c0000-c000-c000-c000-c0000-c00-c0

000000000046}\treatas

000000000046}\inprocserver32

HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprocserver32 Opens key:

HKCU\software\classes\clsid\{00020424-0000-0000-c000-Opens key:

00000000046}\inprocserverx86

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

Opens kev: HKCU\software\microsoft\internet explorer\services Opens key: HKLM\software\microsoft\internet explorer\services

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

 $\label{localization} \begin{tabular}{ll} HKCU \software \mbox{$\stackrel{\cdot}{m}$ icrosoft \internet explorer \activities} \end{tabular}$ Opens key: HKLM\software\microsoft\internet explorer\activities Opens key:

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

explorer\infodelivery\restrictions

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

explorer\infodelivery\restrictions

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

Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-

00000000046}\localserver32

HKCR\clsid\{00020424-0000-0000-c000-00000000046}\localserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-

00000000046}\inprochandler32

Opens key:

HKCU\software\classes\clsid\{00020424-0000-0000-c000-Opens key:

00000000046}\inprochandlerx86

Opens key: HKCU\software\microsoft\internet explorer\suggested sites

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\setupapi.dll

Opens key: HKLM\system\currentcontrolset\control\minint

Opens key: HKLM\system\wpa\pnp

HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprochandlerx86 Opens kev:

Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-

00000000046}\localserver

HKCR\clsid\{00020424-0000-0000-c000-00000000046}\localserver Opens key:

Opens key: HKLM\software\microsoft\windows\currentversion\setup

Opens key: HKLM\software\microsoft\windows\currentversion\setup\apploglevels

HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-Opens key:

0080c7f4ee85}\forward

Opens key: HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\forward Opens key: HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-

0080c7f4ee85}\typelib

Opens key: HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \typelib \end{tabular} $$ \{eab 22 a c 0 - 30 c 1 - 11 c f - a 7 e b - 000 0 c 05 b a e 0 b \} $$ \end{tabular} $$ A c b - 10 c f - a 7 e b - 000 0 c 05 b a e 0 b \} $$ \end{tabular} $$ A c b - 10 c f - a 7 e b - 000 0 c 05 b a e 0 b \} $$ \end{tabular} $$ A c b - 10 c f - a 7 e b - 000 0 c 05 b a e 0 b \} $$ \end{tabular} $$ A c b - 10 c f - a 7 e b - 000 0 c 05 b a e 0 b \} $$ \end{tabular} $$ A c b - 10 c f - a 7 e b - 000 0 c 05 b a e 0 b \} $$ \end{tabular} $$ A c b - 10 c f - a 7 e b - 000 0 c 05 b a e 0 b \} $$ \end{tabular} $$ A c b - 10 c f - a 7 e b - 000 0 c 05 b a e 0 b \} $$ \end{tabular} $$ A c b - 10 c f - a 7 e b - 000 0 c 05 b a e 0 b \} $$ \end{tabular} $$ A c b - 10 c f - a 7 e b - 000 0 c 05 b a e 0 b \} $$ \end{tabular} $$ A c b - 10 c f - a 7 e b - 000 0 c 05 b a e 0 b \} $$ \end{tabular} $$ A c b - 10 c f - a 7 e b - 000 0 c 05 b a e 0 b \} $$ \end{tabular} $$ A c b - 10 c f - a 7 e b - 000 0 c 05 b a e 0 b \} $$ \end{tabular} $$ A c b - 10 c f - a 7 e b - 000 0 c 05 b a e 0 b \} $$ \end{tabular} $$ A c b - 10 c f - a 7 e b - 000 0 c 05 b a e 0 b \} $$ \end{tabular} $$ A c b - 10 c f - a 7 e b - 000 0 c 05 b a e 0 b \} $$ \end{tabular} $$ A c b - 10 c f - a 7 e b - 000 0 c 05 b a e 0 b \} $$ \end{tabular} $$ A c b - 10 c f - a 7 e b - 000 0 c 05 b a e 0 b \} $$ \end{tabular} $$ A c b - 10 c f - a 7 e b - 000 0 c 05 b a e 0 b \} $$ \end{tabular} $$ A c b - 10 c f - a 7 e b - 000 0 c 05 b a e 0 b A c b - 000$

Opens key: HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}

Opens key: HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1

HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1 Opens key: Opens key: HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-

0000c05bae0b}\1.1\0

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ \ explorer \ \ mountpoints 2 \ \ cpc \ \ \ volume$

Opens kev:

11e3-9fc7-806d6172696f}\

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 kev: HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32

HKCU\software\classes\directory Opens key:

Opens key: HKCR\directory

Opens key: HKCU\software\classes\directory\curver

HKCR\directory\curver Opens key: Opens key: HKCR\directory\

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

Opens key:

Opens key: HKCU\software\classes\interface\{00020400-0000-0000-c000-

00000000046}\proxystubclsid32

Opens key: HKCR\interface\{00020400-0000-0000-c000-00000000046}\proxystubclsid32 Opens key: HKCU\software\microsoft\windows\currentversion\policies\system HKCU\software\classes\clsid\{00020420-0000-0000-c000-00000000046} Opens key:

Opens key: HKCR\clsid\{00020420-0000-0000-c000-00000000046} Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-

000000000046}\treatas

Opens key: HKCR\clsid\{00020420-0000-0000-c000-00000000046}\treatas Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-

00000000046}\inprocserver32

Opens key: HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprocserver32

HKCU\software\classes\clsid\{00020420-0000-0000-c000-Opens kev:

00000000046}\inprocserverx86

Opens key: HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprocserverx86

HKCU\software\classes\clsid\{00020420-0000-0000-c000-Opens key:

00000000046}\localserver32

Opens key: HKCR\clsid\{00020420-0000-0000-c000-00000000046}\localserver32

HKCU\software\classes\directory\shellex\iconhandler Opens kev: Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{00020420-0000-0000-c000-c000-c000-c000-c0000-c00-c00-c000-c000-c00-c00-c000-c00-$ 00000000046}\inprochandler32

HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprochandler32 Opens kev:

HKCU\software\classes\clsid\{00020420-0000-0000-c000-Opens kev:

00000000046}\inprochandlerx86

Opens key: HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-

000000000046}\localserver

Opens key: HKCR\clsid\{00020420-0000-0000-c000-00000000046}\localserver

HKCR\directory\shellex\iconhandler Opens key: Opens key: HKCU\software\classes\directory\clsid

Opens key: HKCR\directory\clsid

HKCU\software\classes\folder Opens key:

Opens key: HKCR\folder

HKCU\software\classes\folder\clsid Opens key:

HKCR\folder\clsid Opens key:

HKCU\software\classes\interface\{6d5140c1-7436-11ce-8034-00aa006009fa} Opens key:

Opens key: HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa} Opens key: HKCU\software\classes\interface\{6d5140c1-7436-11ce-8034-

00aa006009fa}\proxystubclsid32

HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32 Opens key: Opens key: HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}

HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9} Opens key: Opens key: HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-

00a0c90dcaa9}\treatas

Opens key: $HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\$ \treatas HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-Opens key:

00a0c90dcaa9}\inprocserver32

Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}

HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000} Opens kev:

Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\shell

Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\shell $HKCU \setminus software \setminus classes \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - c2a7 - c$ Opens key:

444553540000}\shellex\iconhandler

Opens key: HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprocserver32

Opens kev:

00a0c90dcaa9}\inprocserverx86

Opens key: HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-

00a0c90dcaa9}\localserver32

Opens key: HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\localserver32 Opens key: $HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\shellex\iconhandler$ Opens key:

Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\clsid HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-Opens key:

00a0c90dcaa9}\inprochandler32

Opens key: HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprochandler32

HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-Opens key:

00a0c90dcaa9}\inprochandlerx86

HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprochandlerx86 Opens kev:

HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-Opens key:

00a0c90dcaa9}\localserver

HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\localserver Opens key:

HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-Opens key:

444553540000}\inprocserver32

Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32 HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key:

options\actxprxy.dll

HKCU\software\classes\interface\{00020404-0000-0000-c000-000000000046} Opens key:

HKCR\interface\{00020404-0000-0000-c000-00000000046} Opens key: Opens key: HKCU\software\classes\interface\{00020404-0000-0000-c000-

000000000046}\proxystubclsid32

HKCR\interface\{00020404-0000-0000-c000-00000000046}\proxystubclsid32 Opens key:

Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-

444553540000}\treatas

Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\treatas

Opens key: HKCU\software\classes\clsid\{00020421-0000-0000-c000-00000000046}

Opens key: HKCR\clsid\{00020421-0000-0000-c000-00000000046} Opens key:

000000000046}\treatas Opens key:

HKCR\clsid\{00020421-0000-0000-c000-00000000046}\treatas HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-Opens key:

444553540000}\inprocserverx86

Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserverx86

HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-Opens key:

444553540000}\localserver32

Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\localserver32

Opens key: HKCU\software\classes\clsid\{00020421-0000-0000-c000-

000000000046}\inprocserver32

Opens key: HKCR\clsid\{00020421-0000-0000-c000-00000000046}\inprocserver32

HKCU\software\classes\clsid\{00020421-0000-0000-c000-Opens key:

000000000046}\inprocserverx86

HKCR\clsid\{00020421-0000-0000-c000-00000000046}\inprocserverx86 Opens kev:

Opens key: HKCU\software\classes\clsid\{00020421-0000-0000-c000-

```
00000000046}\localserver32
                                                                      HKCR\clsid\{00020421-0000-0000-c000-00000000046}\localserver32
     Opens kev:
                                                                       HKCU\software\classes\clsid\{00020421-0000-0000-c000-
     Opens kev:
00000000046}\inprochandler32
     Opens key:
                                                                       HKCR\clsid\{00020421-0000-0000-c000-00000000046}\inprochandler32
                                                                       HKCU\software\classes\clsid\{00020421-0000-0000-c000-
     Opens key:
 000000000046}\inprochandlerx86
                                                                      HKCR\clsid\{00020421-0000-0000-c000-00000000046}\inprochandlerx86
     Opens key:
                                                                      HKCU\software\classes\clsid\{00020421-0000-0000-c000-
     Opens key:
00000000046}\localserver
     Opens kev:
                                                                      HKCR\clsid\{00020421-0000-0000-c000-00000000046}\localserver
     Opens key:
                                                                       HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
 444553540000}\inprochandler32
                                                                      HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandler32
     Opens key:
                                                                       HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
     Opens key:
444553540000}\inprochandlerx86
     Opens key:
                                                                      HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandlerx86
     Opens key:
                                                                      HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
 444553540000}\localserver
                                                                      HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\localserver
     Opens key:
     Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{ff393560-c2a7-11cf-
bff4-444553540000}
     Opens key:
                                                                       HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\mshist012016042220160423
     Opens key:
                                                                      HKCU\software\microsoft\internet explorer\main\windowssearch
     Opens key:
                                                                       HKLM\software\policies\microsoft\internet explorer\feeds
     Opens key:
                                                                       HKCU\software\microsoft\internet explorer\feeds
     Opens key:
                                                                       HKLM\software\microsoft\internet explorer\feeds
     Opens key:
                                                                       HKCU\software\classes\.url\persistenthandler
     Opens key:
                                                                       HKCR\.url\persistenthandler
                                                                       HKLM\software\policies\microsoft\internet explorer\main\windowssearch
     Opens key:
     Opens key:
                                                                       HKLM\software\microsoft\windows search
     Opens key:
                                                                      HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder
     Opens key:
                                                                       HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder
     Opens key:
                                                                       HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus explorer \setminus clsid \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus clsid \setminus 
 3aea-1069-a2d8-08002b30309d}
     Opens key:
                                                                       HKCU\software\microsoft\windows\currentversion\policies\nonenum
     Opens key:
                                                                       HKLM\software\microsoft\windows\currentversion\policies\nonenum
                                                                       HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-theoryte \} + theoryte \setminus foreign + theoryte \}
     Opens key:
 3aea-1069-a2d8-08002b30309d}\shellfolder
     Opens key:
                                                                      HKLM \setminus software \setminus icrosoft \setminus windows \setminus current version \setminus explorer \setminus (20d04feo-block) + 
 3aea-1069-a2d8-08002b30309d}\shellfolder
     Opens key:
                                                                       HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
     Opens key:
                                                                       HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
                                                                       HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\
     Opens key:
     Opens key:
                                                                       HKCU\software\microsoft\windows\shellnoroam
                                                                       HKCU\software\microsoft\windows\shellnoroam\muicache
     Opens kev:
                                                                       HKCU\software\microsoft\windows\shellnoroam\muicache\
     Opens key:
     Opens key:
                                                                       HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}
     Opens key:
                                                                       HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}
     Opens key:
                                                                       HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
 0000f81fe221}\treatas
     Opens kev:
                                                                       HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\treatas
                                                                      HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
     Opens key:
0000f81fe221}\inprocserver32
                                                                      HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprocserver32
     Opens key:
                                                                       HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
     Opens key:
0000f81fe221}\inprocserverx86
     Opens key:
                                                                       HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprocserverx86
     Opens key:
                                                                      HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\localserver32
     Opens key:
                                                                       HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\localserver32
                                                                       HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
     Opens key:
0000f81fe221}\inprochandler32
     Opens key:
                                                                      HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprochandler32
                                                                      HKCU \setminus software \setminus classes \setminus clsid \setminus \{f5078f35 - c551 - 11d3 - 89b9 - f13f - f
     Opens key:
0000f81fe221}\inprochandlerx86
     Opens key:
                                                                      HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprochandlerx86
                                                                      HKCU\software\classes\clsid\{f5078f35-c551-11d3-89b9-
     Opens key:
 0000f81fe221}\localserver
     Opens key:
                                                                      HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\localserver
                                                                       HKCU\software\classes\shockwaveflash.shockwaveflash.7
     Opens key:
     Opens key:
                                                                       HKCR\shockwaveflash.shockwaveflash.7
```

HKCU\software\classes\shockwaveflash.shockwaveflash.7\clsid Opens kev: HKCR\shockwaveflash.shockwaveflash.7\clsid Opens key: Opens key: HKCU\software\classes\mime\database\content type\image/x-icon Opens key: HKCR\mime\database\content type\image/x-icon Opens key: HKCU\software\classes\protocols\filter\image/x-icon Opens key: HKCR\protocols\filter\image/x-icon Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_mime_treat_image_as_authoritative

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_mime_treat_image_as_authoritative

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

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-47f3-893f-47f3-893f-47f3-893f-47f3-893f-47f3-893f-47f3-893f-47f3-893f-47f3-895f-47f3-895f-47f3-895f-47f3-895f-47f3-895f-47f3-895f-47f3-895f-47f3-895f-47f3-895f-47f3-895f-47f3-895f-47f-47f-47f-4

fd2b31b3eefd}\treatas

Opens key: $\label{eq:hccn} \begin{tabular}{ll} HKCR\clsid\{e}569bde7-a8dc-47f3-893f-fd2b31b3eefd}\treatas \\ Opens key: \\ HKCU\software\classes\clsid\{e}569bde7-a8dc-47f3-893f-\\ \end{tabular}$

fd2b31b3eefd}\inprocserver32

Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32

Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\inprocserverx86

Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\localserver32

Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\localserver32

Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\inprochandler32

Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprochandler32

Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\inprochandlerx86

Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\localserver

Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\localserver

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

compatibility\{adc6cb82-424c-11d2-952a-00c04fa34f05}

Opens key: HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}

Opens key: HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05} Opens key: HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-

00c04fa34f05}\treatas

Opens key: HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\treatas
Opens key: HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-

00c04fa34f05}\inprocserver32

Opens key: HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\inprocserver32

Opens key: HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-

00c04fa34f05}\inprocserverx86

Opens key: HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-

00c04fa34f05}\localserver32

Opens key: HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\localserver32

Opens key: HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-

00c04fa34f05}\inprochandler32

 $Opens~key: \\ HKCR\clsid\\{adc6cb82-424c-11d2-952a-00c04fa34f05}\\{inprochandler32}$

Opens key: HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-

Opens key: HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{adc6cb82-424c-11d2-952a-

00c04fa34f05}\localserver

Opens key: HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\localserver Opens key: HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}

Opens key: HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}
Opens key: HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-

00c04fd9189d}\treatas

Opens key: HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\treatas Opens key: HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-

00c04fd9189d}\inprocserver32

Opens key: HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32

Opens key: HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-

00c04fd9189d}\inprocserverx86

Opens key: HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-

00c04fd9189d}\localserver32

 $Opens~key: \\ HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\localserver 32$

Opens key: $\label{lem:hkcusoftware} \ \ \, \text{HKCU} \\ \ \, \text{HKCU} \\ \ \ \, \text{HKCU} \\ \ \ \, \text{HKCU} \\ \ \ \, \text{HKCU$

00c04fd9189d}\inprochandler32

Opens key: HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprochandler32

Opens key: HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-

 ${\tt 00c04fd9189d} \verb|\inprochandlerx86| \\$

 $Opens~key: \\ HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\ \ inprochandler x86 \\$

Opens key: HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-

00c04fd9189d}\localserver

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]

Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]

Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\microsoft\windows

nt\currentversion\compatibility32[1af5338669efabe0a9841478396871b1]

Queries value: HKLM\software\microsoft\windows nt\currentversion\ime

```
compatibility[1af5338669efabe0a9841478396871b1]
                         HKLM\software\microsoft\windows nt\currentversion\windows[appinit dlls]
 Oueries value:
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
 Queries value:
                         HKLM\system\setup[systemsetupinprogress]
 Oueries value:
                         HKCU\control panel\desktop[multiuilanguageid]
 Queries value:
                         HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
                         HKLM\software\microsoft\ole[rwlockresourcetimeout]
 Oueries value:
 Oueries value:
                         HKCR\interface[interfacehelperdisableall]
                         HKCR\interface[interfacehelperdisableallforole32]
 Oueries value:
 Oueries value:
                         HKCR\interface[interfacehelperdisabletypelib]
 Queries value:
                         HKCR\interface\{00020400-0000-0000-c000-
00000000046}[interfacehelperdisableall]
                         HKCR\interface\{00020400-0000-0000-c000-
 Oueries value:
00000000046}[interfacehelperdisableallforole32]
                         HKCU\control panel\desktop[smoothscroll]
 Queries value:
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
                         HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_protocol_lockdown[1af5338669efabe0a9841478396871b1.exe]
                         HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_protocol_lockdown[*]
 Queries value:
                         HKLM\software\microsoft\ctf\systemshared[cuas]
 Oueries value:
                         HKCU\keyboard layout\toggle[language hotkey]
 Queries value:
                         HKCU\keyboard layout\toggle[hotkey]
 Queries value:
                         HKCU\keyboard layout\toggle[layout hotkey]
 Oueries value:
                         HKLM\software\microsoft\ctf[enableanchorcontext]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
 Queries value:
                         HKCU\control panel\desktop[lamebuttontext]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
 Queries value:
                         HKCU\software\microsoft\ctf[disable thread input manager]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\fontsubstitutes[tahoma]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
shell dlg]
 Oueries value:
                         HKLM\software\microsoft\ole[maximumallowedallocationsize]
 Queries value:
                         HKLM\software\microsoft\com3[com+enabled]
 Queries value:
                         HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
 Oueries value:
                         {\tt HKLM \setminus software \setminus microsoft \setminus ole[minimumfreemempercentage to create object]}
                         HKLM\software\microsoft\com3[regdbversion]
 Queries value:
                         HKCR\clsid\{8856f961-340a-11d0-a96b-
 Oueries value:
00c04fd705a2}\inprocserver32[inprocserver32]
                         HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32[]
 Oueries value:
 Queries value:
                         HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[appid]
 Oueries value:
                         HKCR\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[threadingmodel]
                         HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe[]
 Oueries value:
 Queries value:
                         HKLM\software\microsoft\internet explorer\setup[iexplorelastmodifiedlow]
                         HKLM\software\microsoft\internet
 Oueries value:
explorer\setup[iexplorelastmodifiedhigh]
 Queries value:
                         HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
ab78-1084642581fb]
 Oueries value:
                         HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
0000-0000000000000
 Oueries value:
                         HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
                         HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib[]
 Oueries value:
 Queries value:
                         HKLM\software\microsoft\internet explorer\setup[installstarted]
 Queries value:
                         HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32[]
 Oueries value:
                         HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32[]
                         HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32[]
 Queries value:
 Queries value:
                         Oueries value:
                         HKLM\software\microsoft\rpc[maxrpcsize]
 Oueries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
                         HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[createuricachesize]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablepunycode]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
 Oueries value:
                         HKCU\software\microsoft\internet explorer\ietldfietlddllversionlowl
 Queries value:
                         HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
                         HKCU\software\microsoft\internet explorer\main[frametabwindow]
 Oueries value:
 Oueries value:
                         HKLM\software\microsoft\internet explorer\main[frametabwindow]
 Oueries value:
                         HKCU\software\microsoft\internet explorer\main[framemerging]
 Queries value:
                         HKLM\software\microsoft\internet explorer\main[framemerging]
                         HKCU\software\microsoft\internet explorer\main[sessionmerging]
 Oueries value:
 Queries value:
                         HKLM\software\microsoft\internet explorer\main[sessionmerging]
```

```
HKCU\software\microsoft\internet explorer\main[admintabprocs]
  Oueries value:
  Oueries value:
                                        HKLM\software\microsoft\internet explorer\main[admintabprocs]
  Oueries value:
                                        HKLM\software\policies\microsoft\internet explorer\main[tabprocgrowth]
                                        HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
  Queries value:
                                        HKLM\software\microsoft\internet explorer\main[tabprocgrowth]
  Oueries value:
  Queries value:
                                        HKLM\software\microsoft\internet explorer\main[navigationdelay]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonethood]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
  Queries value:
                                        HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[]
  Oueries value:
                                        HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[loadwithoutcom]
  Queries value:
                                        HKLM\software\microsoft\windows\currentversion\shell
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
                                        HKCU\software\microsoft\windows\currentversion\shell
  Queries value:
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[enforceshellextensionsecurity]
                                        HKLM\software\microsoft\windows\currentversion\shell
  Queries value:
0x4011
  Queries value:
                                        HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}}
0x4011
                                        HKLM\system\currentcontrolset\control\session
  Queries value:
manager\appcompatibility[disableappcompat]
                                        HKCR\clsid\{871c5380-42a0-1069-a2ea-
  Queries value:
08002b30309d}\inprocserver32[inprocserver32]
  Queries value:
                                        HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[appid]
  Oueries value:
                                        HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[threadingmodel]
                                        HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[fromcachetimeout]
                                        HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[secureprotocols]
                                        HKLM\software\policies\microsoft\internet
  Queries value:
explorer\main[security_hklm_only]
                                        HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[certificaterevocation]
  Oueries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
  Queries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
                                        HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[idnenabled]
                                        HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[cachemode]
  Queries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
                                        HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[proxyhttp1.1]
  Queries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
                                        \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
  Queries value:
settings[disablebasicoverclearchannel]
                                        HKCU\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
                                        HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
  Queries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
                                        HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[syncmode5]
  Queries value:
                                        \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
  Queries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[signature]
                                        HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\content[peruseritem]
  Queries value:
                                        \label{lem:hklm} \mbox{HKLM} \mbox{$\tt MKLM} \mbox
settings\5.0\cache\content[peruseritem]
  Queries value:
                                        HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
                                        HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\content[cacheprefix]
  Queries value:
                                        \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\content[cachelimit]
```

 $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} in the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu$

Queries value:

```
settings\5.0\cache\cookies[peruseritem]
                          HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\cookies[peruseritem]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
 Queries value:
                          \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\cookies[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\cookies[cachelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
 Queries value:
                          \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
settings\5.0\cache\history[peruseritem]
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Oueries value:
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]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cacheoptions]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cachepath]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachepath]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cachelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\ietld[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\ietld[cacheprefix]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\ietld[cacheoptions]
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
                          \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current version \+ internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
```

HKCU\software\microsoft\windows\currentversion\internet

Oueries value:

settings\5.0\cache\extensible cache\privacie:[cachepath]

```
Oueries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[disableworkerthreadhibernation]
                                                  HKLM\software\microsoft\windows\currentversion\internet
   Queries value:
settings[disableworkerthreadhibernation]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[disablereadrange]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[socketsendbufferlength]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[socketreceivebufferlength]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[keepalivetimeout]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[maxhttpredirects]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[maxconnectionsperserver]
                                                  HKLM\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[maxconnectionsperserver]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[maxconnectionsper1_0server]
                                                  HKLM\software\microsoft\windows\currentversion\internet
   Queries value:
settings[maxconnectionsper1 Oserver]
   Oueries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
                                                  HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[serverinfotimeout]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[connecttimeout]
   Queries value:
                                                  HKLM\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[connectretries]
                                                  HKLM\software\microsoft\windows\currentversion\internet
   Queries value:
settings[connectretries]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
                                                  HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[sendtimeout]
   Oueries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
   Queries value:
                                                  HKLM\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[disablentlmpreauth]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
                                                  HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache[scavengecachefilelifetime]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
   Oueries value:
                                                  HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[httpdefaultexpirytimesecs]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirvtimesecs]
   Queries value:
                                                  HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[1af5338669efabe0a9841478396871b1.exe]
                                                  HKLM\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
   Queries value:
                                                  \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
settings[disablecachingofsslpages]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[leashlegacycookies]
   Queries value:
                                                  \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[disablent4rascheck]
   Queries value:
                                                  \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings[dialupuselansettings]
                                                  HKLM\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[dialupuselansettings]
   Queries value:
                                                  \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} in the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu
settings[sendextracrlf]
   Queries value:
                                                  \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} in the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu
```

```
settings[bypassftptimecheck]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[releasesocketduringauth]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
  Queries value:
                                    \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
settings[releasesocketduring401auth]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[wpadsearchalldomains]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
  Queries value:
                                    \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
settings[disablelegacypreauthasserver]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                                    HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasshttpnocachecheck]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
                                    HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasssslnocachecheck]
                                    HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[enablehttptrace]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[nocheckautodialoverride]
                                    \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
  Queries value:
settings[nocheckautodialoverride]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                                    HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dontusednsloadbalancing]
                                    HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[sharecredswithwinhttp]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[headerexclusionlistforcache]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dnscacheentries]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dnscachetimeout]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnalwaysonpost]
                                    \label{lem:hkcu} \verb+KKCU \software \verb+microsoft + windows \verb+current version \verb+\internet+ in the lemma + the lemma 
  Queries value:
settings[warnonzonecrossing]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertsending]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonbadcertrecving]
  Queries value:
                                    \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[warnonpostredirect]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonhttpstohttpredirect]
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000003[packedcatalogitem]
  Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[packedcatalogitem]
  Oueries value:
```

Oueries value:

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[displaystring] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 00000000000003 \ [displaystring] \ Queries \ value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace] Queries value:

 $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace_catalog5 \catalog_entries \namespace_catalog5 \catalog5 \$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[globaluseroffline]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[enableautodial]

Queries value: HKLM\software\microsoft\windows\currentversion\internet

settings[urlencoding]

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

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

Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nofilemenu]

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

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[urlencoding]

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

explorer\security[disablesecuritysettingscheck]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\zones\0[flags]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\zones\1[flags]

```
Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[flags]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[flags]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\zones\4[flags]
  Queries value:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[1af5338669efabe0a9841478396871b1.exe]
  Queries value:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
  Oueries value:
                                  HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[1af5338669efabe0a9841478396871b1.exe]
  Oueries value:
                                  HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
  Oueries value:
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
  Oueries value:
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
  Queries value:
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
  Oueries value:
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
  Queries value:
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
  Queries value:
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
                                   \label{lem:hklm} \mbox{HKLM\software\mbox{\sc mixer1}} \mbox{ $n$-current version\drivers} \mbox{\sc mixer1} \mbox{\sc mixer1} \mbox{\sc mixer2} \mbox{\sc
  Queries value:
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer51
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer81
  Oueries value:
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32maxnumrequestretries]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32requestretrytimeout]
  Queries value:
                                   HKLM\software\microsoft\tracing[enableconsoletracing]
  Oueries value:
                                   HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
                                   HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
  Queries value:
  Oueries value:
                                   HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
  Oueries value:
                                   HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
                                   HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
  Oueries value:
  Queries value:
                                   HKLM\software\microsoft\tracing\rasapi32[filedirectory]
  Queries value:
                                   \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ user shell
folders[common appdata]
                                   HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\winlogon[userenvdebuglevel]
                                   HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\winlogon[chkaccdebuglevel]
  Queries value:
                                   HKLM\system\currentcontrolset\control\productoptions[producttype]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[personal]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local settings]
                                   HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\winlogon[rsopdebuglevel]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
                                   HKLM\software\microsoft\windows
  Oueries value:
```

nt\currentversion\profilelist[profilesdirectory]

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\profilelist[allusersprofile]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\profilelist[defaultuserprofile]

Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir]
Queries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir]

Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

1757981266-507921405-1957994488-1003[profileimagepath]
Queries value: HKCU\software\microsoft\windows

nt\currentversion\winlogon[parseautoexec]

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[appdata]

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]

Oueries value: HKCU\software\microsoft\windows\currentversion\internet

settings\connections[savedlegacysettings]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\connections[defaultconnectionsettings]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap[autodetect]

Queries value: HKCU\software\microsoft\internet explorer[no3dborder]
Queries value: HKLM\software\microsoft\internet explorer[no3dborder]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_mime_handling[1af5338669efabe0a9841478396871b1.exe]

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

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\user agent[]

Queries value: HKLM\software\microsoft\windows\currentversion\internet

settings\5.0\user agent[]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\user agent[compatible]

Queries value: HKLM\software\microsoft\windows\currentversion\internet

settings\5.0\user agent[compatible]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\user agent[version]

Oueries value: HKLM\software\microsoft\windows\currentversion\internet

settings\5.0\user agent[version]

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

agent]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\user agent[platform]

 $\label{thm:linear} Queries \ value: \\ HKLM \ software \ microsoft \ windows \ current version \ internet$

settings\5.0\user agent[platform]

Queries value: HKLM\software\microsoft\internet

 $explorer \verb|\main| featurecontrol| feature_max connections perserver [1af5338669efabe0a9841478396871b1.exe]| feature_max connections perserver [1af5338669efabe0a98841478396871b1.exe]| feature_max connections perserver [1af5338669efabe0a98871b1.exe]| feature_max connections perserver [1af533869efabe0a98871b1.exe]| feature_max connections perserver [1af533869efabe0a98871b1.exe]| feature_max connections perserver [1af533869efabe0a98871b1.exe]| feature_max connections$

Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[*]
Oueries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_maxconnectionsper1_0server[1af5338669efabe0a9841478396871b1.exe]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_maxconnectionsper1_0server[*]

Queries value: HKCU\software\microsoft\internet explorer\international[acceptlanguage]
Queries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]

Queries value:

 $HKLM \verb|\system| current control set \verb|\services| tcpip \verb|\parameters| winsock [used elayed acceptance] \\$

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[append completion]

Queries value:

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]

Queries value: HKCR\clsid\{00bb2765-6a77-11d0-a535-

00c04fd7d062}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]

Queries value: $\label{eq:hkcr} \begin{tabular}{ll} HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\{[appid]} \end{tabular}$

Queries value: HKCR\clsid\{00bb2765-6a77-11d0-a535-

```
00c04fd7d062}\inprocserver32[threadingmodel]
                        HKCR\clsid\{6935db93-21e8-4ccc-beb9-
 Oueries value:
9fe3c77a297a}\inprocserver32[inprocserver32]
                        HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\inprocserver32[]
 Queries value:
 Oueries value:
                        HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}[appid]
 Queries value:
                       HKCR\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprocserver32[threadingmodel]
                       HKCU\software\microsoft\windows\currentversion\explorer\runmru[mrulist]
 Oueries value:
 Oueries value:
                        HKCU\software\microsoft\windows\currentversion\explorer\runmru[c]
                        HKCU\software\microsoft\windows\currentversion\explorer\runmru[b]
 Oueries value:
 Oueries value:
                        HKCU\software\microsoft\windows\currentversion\explorer\runmru[a]
 Queries value:
                        HKCR\clsid\{00bb2764-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
                       HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
 Oueries value:
 Oueries value:
                        HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}[appid]
                        HKCR\clsid\{00bb2764-6a77-11d0-a535-
 Oueries value:
00c04fd7d062}\inprocserver32[threadingmodel]
 Queries value:
                        HKCR\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
                       HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
 Oueries value:
 Queries value:
                        HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}[appid]
 Queries value:
                        HKCR\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
 Queries value:
                        HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32[]
 Oueries value:
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewscrollover]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\advanced[listviewscrollover]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewwatermark]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewalphaselect]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
                        HKLM\software\microsoft\rpc\securityservice[10]
 Queries value:
 Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
                        HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
 Queries value:
 Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]
 Oueries value:
                        HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]
 Queries value:
HKLM\svstem\currentcontrolset\control\lsa\sspicache\msapsspc.dll[version]
                        Queries value:
 Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]
 Queries value:
                        HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]
 Queries value:
 Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities]
                        HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid]
 Queries value:
 Queries value:
                        HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version]
                        HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize]
                        HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name]
 Oueries value:
                        HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment]
 Queries value:
 Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities]
                        HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid]
 Oueries value:
 Queries value:
                        HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version]
 Oueries value:
                        HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type]
HKLM\system\currentcontrol\set\control\lsa\sspicache\msnsspc.dll[tokensize]
                        HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
 Queries value:
                        HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\3[1a10]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [prioritize record data]
```

Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] Oueries 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] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [register wan adapters]$ Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Queries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones] Oueries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[dnstest] HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel] HKLM\svstem\currentcontrolset\services\dnscache\parameters[multicastsendlevel] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts] Oueries value: HKLM\svstem\currentcontrolset\services\tcpip\parameters[dnsmulticastguerytimeouts] Oueries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind] Queries value: c7d49d7cecdc}[enabledhcp]

```
Oueries value:
```

 $\label{lem:hklm} HKLM \ system \ `corrent controlset \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [lease obtained time]$

Oueries value

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [lease terminates time]$

Queries value:

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

Queries value:

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[disableadapterdomainname]

Queries value:

 $\label{lem:hklmsystem} HKLM \system \criteriaces \true \are \criteriaces \finterfaces \finterf$

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [register adapter name]$

Queries value:

 $HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [registration maxaddress count]$

Queries value:

 $\label{local-equation} HKLM \system \current control set \services \troip \parameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [maxnumber of addresses to register]$

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[domain]

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \troip \parameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [dhcpdomain]$

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \troip \parameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [ipautoconfiguration enabled]$

Oueries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [addresstype]$

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [nameserver]$

Queries value:

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

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [dnsnbtlook upor der]$

 $\label{thm:linear} Queries \ value: \\ HKLM\software\mbox{\mbox{$^$microsoft\cryptography\defaults\provider\mbox{\mbox{$microsoft\ strong}$}}$

cryptographic provider[image path]

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

Queries value: HKCU\software\microsoft\internet

explorer\ietld\lowmic[ietlddllversionlow]

Queries value: HKCU\software\microsoft\internet

explorer\ietld\lowmic[ietlddllversionhigh]

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]

 $\label{lem:content_type} Queries \ value: \qquad \qquad \text{HKCR} \\ \text{mime} \\ \text{database} \\ \text{content_type} \\ \text{text/html[extension]}$

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_mime_sniffing[1af5338669efabe0a9841478396871b1.exe]

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

 $\label{thm:condition} Queries \ value: \\ HKCU \ software \ microsoft \ windows \ current version \ internet$

settings[istextplainhonored]

explorer\main\featurecontrol\feature_feeds[1af5338669efabe0a9841478396871b1.exe]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_feeds[*]

Queries value: HKLM\software\microsoft\internet

 $\verb|explorer| a in feature control feature_safe_bind to object[1af5338669 efabe0a 9841478396871b1.exe]|$

Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_safe_bindtoobject[*] Queries value: HKCR\clsid\{25336920-03f9-11cf-8fd0-

00aa00686f13}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[]

Queries value: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[appid]

Queries value: HKCR\clsid\{25336920-03f9-11cf-8fd0-

00aa00686f13}\inprocserver32[threadingmodel] HKLM\software\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_legacy_dispparams[1af5338669efabe0a9841478396871b1.exe] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_legacy_dispparams[*] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_object_caching[1af5338669efabe0a9841478396871b1.exe] Oueries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_object_caching[*] HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay] Oueries value: HKLM\software\microsoft\internet explorer\application Oueries value: compatibility[1af5338669efabe0a9841478396871b1.exe] Oueries value: HKCU\software\microsoft\internet explorer\domstorage[totallimit] HKCU\software\microsoft\internet explorer\domstorage[domainlimit] Oueries value: Oueries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragscrollinset] HKCU\software\microsoft\windows Oueries value: nt\currentversion\windows[dragscrolldelay] Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragscrollinterval] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_filedownload[1af5338669efabe0a9841478396871b1.exe] Oueries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_filedownload[*] Queries value: HKCR\protocols\handler\about[clsid] Oueries value: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[inprocserver32] Queries value: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[] HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}[appid] Oueries value: Queries value: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[threadingmodel] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\3[2106] Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\3[2106] Queries value: HKCU\software\microsoft\internet explorer\zoom[zoomdisabled] Queries value: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[] HKCU\software\microsoft\windows\currentversion\internet settings\url Oueries value: history[daystokeep] Queries value: HKLM\software\policies\microsoft\internet explorer[smartdithering] HKCU\software\microsoft\internet explorer[smartdithering] Oueries value: Queries value: HKCU\software\microsoft\internet explorer[rtfconverterflags] Queries value: HKLM\software\policies\microsoft\internet explorer\main[usecleartype] ${\tt HKCU \setminus software \setminus microsoft \setminus internet \ explorer \setminus main[useclear type]}$ Oueries value: HKLM\software\policies\microsoft\internet Oueries value: explorer\main[page_transitions] HKCU\software\microsoft\internet explorer\main[page_transitions] Queries value: Queries value: HKLM\software\policies\microsoft\internet explorer\main[use_dlgbox_colors] HKCU\software\microsoft\internet explorer\main[use_dlgbox_colors] Queries value: Queries value: HKLM\software\policies\microsoft\internet explorer\main[anchor underline] HKCU\software\microsoft\internet explorer\main[anchor underline] Oueries value: HKCU\software\microsoft\internet explorer\main[css_compat] Queries value: Oueries value: HKCU\software\microsoft\internet explorer\main[expand alt text] Queries value: HKLM\software\policies\microsoft\internet explorer\main[display inline images] Queries value: HKCU\software\microsoft\internet explorer\main[display inline images] Oueries value: HKLM\software\policies\microsoft\internet explorer\main[display inline videos] Queries value: HKCU\software\microsoft\internet explorer\main[display inline videos] HKLM\software\policies\microsoft\internet Oueries value: explorer\main[play_background_sounds] Queries value: HKCU\software\microsoft\internet explorer\main[play_background_sounds] Oueries value: $HKLM \setminus software \setminus policies \setminus microsoft \setminus internet \ explorer \setminus main[play_animations]$ Queries value: HKCU\software\microsoft\internet explorer\main[play_animations] Queries value: HKLM\software\policies\microsoft\internet explorer\main[print_background] Queries value: HKCU\software\microsoft\internet explorer\main[print_background] Queries value: HKCU\software\microsoft\internet explorer\main[use stylesheets] Oueries value: HKLM\software\policies\microsoft\internet explorer\main[smoothscroll] Queries value: HKCU\software\microsoft\internet explorer\main[smoothscroll] Oueries value: HKLM\software\policies\microsoft\internet explorer\main[xmlhttp] Queries value: HKCU\software\microsoft\internet explorer\main[xmlhttp] Queries value: HKLM\software\policies\microsoft\internet explorer\main[show image placeholders1 HKCU\software\microsoft\internet explorer\main[show image placeholders] Queries value: HKLM\software\policies\microsoft\internet explorer\main[disable script Oueries value: debugger] HKCU\software\microsoft\internet explorer\main[disable script debugger] Oueries value:

HKCU\software\microsoft\internet explorer\main[disablescriptdebuggerie]
HKCU\software\microsoft\internet explorer\main[move system caret]

 $\label{lem:hkcu} \verb+KKCU\+ software\+ internet explorer\+ main[force offscreen]$

Queries value:

Queries value: Queries value:

```
composition]
                         HKLM\software\policies\microsoft\internet explorer\main[enable
 Oueries value:
autoimageresize]
                         HKCU\software\microsoft\internet explorer\main[enable autoimageresize]
 Queries value:
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[usethemes]
                         HKCU\software\microsoft\internet explorer\main[usehr]
 Queries value:
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[q300829]
                         HKCU\software\microsoft\internet explorer\main[cleanup htcs]
 Oueries value:
 Oueries value:
                         HKLM\software\policies\microsoft\internet explorer\main[xdomainrequest]
                         HKCU\software\microsoft\internet explorer\main[xdomainrequest]
 Oueries value:
 Oueries value:
                         HKLM\software\microsoft\internet explorer\main[xdomainrequest]
 Queries value:
                         HKLM\software\policies\microsoft\internet explorer\main[domstorage]
 Oueries value:
                         HKCU\software\microsoft\internet explorer\main[domstorage]
                         HKLM\software\microsoft\internet explorer\main[domstorage]
 Oueries value:
 Oueries value:
                         HKCU\software\microsoft\internet
explorer\international[default_codepage]
 Oueries value:
                         HKCU\software\microsoft\internet explorer\international[autodetect]
 Queries value:
                         HKCU\software\microsoft\internet
explorer\international\scripts[default_iefontsizeprivate]
 Oueries 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]
 Oueries 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
hyperlinks1
 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]
                         HKLM\system\currentcontrolset\control\nls\codepage[950]
 Oueries value:
 Queries value:
                         HKCU\software\microsoft\internet
explorer\international\scripts\3[iefontsize]
                         HKCU\software\microsoft\internet
 Oueries value:
explorer\international\scripts\3[iefontsizeprivate]
 Queries value:
                         HKCU\software\microsoft\internet
explorer\international\scripts\3[iepropfontname]
                        HKCU\software\microsoft\internet
 Queries value:
explorer\international\scripts\3[iefixedfontname]
                         HKLM\software\microsoft\internet explorer\version vector[vml]
 Queries value:
                         HKLM\software\microsoft\internet explorer\version vector[ie]
 Oueries value:
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation[1af5338669efabe0a9841478396871b1.exe]
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation[*]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter[1af5338669efabe0a9841478396871b1.exe]
 Oueries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter[*]
                        HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones[securitysafe]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_behaviors[1af5338669efabe0a9841478396871b1.exe]
                         HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_behaviors[*]
                         HKLM\software\microsoft\internet explorer\default behaviors[discovery]
 Queries value:
 Queries value:
                         HKCR\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[inprocserver32]
                         \label{local-bb82-00aa00bdce0b} Linprocserver 32[] \\
 Queries value:
 Queries value:
                         HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}[appid]
                         HKCR\clsid\{3050f4cf-98b5-11cf-bb82-
 Oueries value:
00aa00bdce0b}\inprocserver32[threadingmodel]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown[1af5338669efabe0a9841478396871b1.exe]
 Oueries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown[*]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonintranet]
```

Queries value: HKCR\clsid\{50d5107a-d278-4871-8989-

 $\label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet$

Queries value:

settings[warnonintranet]

```
f4ceaaf59cfc}\inprocserver32[inprocserver32]
                          HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32[]
 Oueries value:
 Oueries value:
                          HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[appid]
 Queries value:
                          HKCR\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[threadingmodel]
 Queries value:
                          HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}[enable]
                          HKCR\clsid\{3ce74de4-53d3-4d74-8b83-
 Oueries value:
431b3828ba53}\inprocserver32[inprocserver32]
                          HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32[]
 Queries value:
                          HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}[appid]
 Oueries value:
 Queries value:
                          HKCR\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprocserver32[threadingmodel]
                          HKCR\clsid\{a4b544a1-438d-4b41-9325-
 Oueries value:
869523e2d6c7}\inprocserver32[inprocserver32]
                          HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserver32[]
 Queries value:
                          HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}[appid]
 Queries value:
 Queries value:
                          HKCR\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprocserver32[threadingmodel]
                          HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
 Queries value:
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}[description]
 Queries value:
                          HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[description]
 Queries value:
                          HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}[description]
                          HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
 Queries value:
00aa00bbbb58}\inprocserver32[inprocserver32]
 Queries value:
                          HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32[]
                          \label{local-equation} $HKCR\clsid{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}[appid]$
 Queries value:
 Queries value:
                          HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[threadingmodel]
                          HKLM\system\currentcontrolset\control\nls\locale[00000409]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\control\nls\language groups[1]
 Queries value:
                          HKLM\software\microsoft\ole[defaultaccesspermission]
 Oueries value:
                          HKLM \verb|\system| current control \verb|\sa[everyone includes an ony mous]|
 Queries value:
                          HKCU\software\microsoft\internet explorer\recovery[autorecover]
 Queries value:
                          HKLM\software\microsoft\internet explorer\default behaviors[homepage]
                          HKCR\clsid\{81397204-f51a-4571-8d7b-
 Oueries value:
dc030521aabd}\inprocserver32[inprocserver32]
                          HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32[]
 Queries value:
                          HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}[appid]
 Oueries value:
                          HKCR\clsid\{81397204-f51a-4571-8d7b-
 Queries value:
dc030521aabd}\inprocserver32[threadingmodel]
                          HKCR\clsid\{d1fe6762-fc48-11d0-883a-
 Queries value:
3c8b00c10000}\inprocserver32[inprocserver32]
 Queries value:
                          HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserver32[]
                          HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}[appid]
 Oueries value:
 Queries value:
                          HKCR\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprocserver32[threadingmodel]
 Queries value:
                          HKLM\software\microsoft\internet explorer\default
behaviors[dxtfilterbehavior]
                          HKCR\clsid\{4fd2a832-86c8-11d0-8fca-
 Oueries value:
00c04fd9189d}\inprocserver32[inprocserver32]
                          \label{local-bound} $$HKCR\clsid_{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32[]$
 Queries value:
 Oueries value:
                          HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}[appid]
 Queries value:
                          HKCR\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocserver32[threadingmodel]
                          HKLM\hardware\devicemap\video[maxobjectnumber]
 Oueries value:
 Oueries value:
                          HKLM\hardware\devicemap\video[\device\video0]
 Queries value:
                          HKLM\hardware\devicemap\video[\device\video1]
 Queries value:
                          HKLM\hardware\devicemap\video[\device\video2]
 Oueries value:
                          HKLM\software\microsoft\directdraw\compatibility\bug![name]
                          HKLM\software\microsoft\directdraw\compatibility\bug![flags]
 Queries value:
 Queries value:
                          HKLM\software\microsoft\directdraw\compatibility\bug![id]
                          HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[name]
 Oueries value:
 Queries value:
                          HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[flags]
 Queries value:
                          HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[id]
                          HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus mortal kombat \\ 3[name]
 Oueries value:
 Queries value:
                          HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[flags]
 Queries value:
                          HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[id]
                          HKLM\software\microsoft\directdraw\compatibility\msgolf98[name]
 Queries value:
                          HKLM\software\microsoft\directdraw\compatibility\msgolf98[flags]
 Oueries value:
 Oueries value:
                          HKLM\software\microsoft\directdraw\compatibility\msgolf98[id]
                          HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus nhlpowerplay [name] \\
 Oueries value:
 Queries value:
                          HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[flags]
                          HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[id]
 Oueries value:
                          HKLM \verb|\software\m| icrosoft \verb|\directdraw\compatibility\nortonsysteminfo[name]|
 Queries value:
                          HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[flags]
 Oueries value:
 Oueries value:
                          HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[id]
 Oueries value:
                          HKLM\software\microsoft\directdraw\compatibility\rogue squadron[name]
 Queries value:
                          HKLM\software\microsoft\directdraw\compatibility\rogue squadron[flags]
 Oueries value:
                          HKLM\software\microsoft\directdraw\compatibility\rogue squadron[id]
 Queries value:
                          HKLM\software\microsoft\directdraw\compatibility\savage[name]
```

```
HKLM\software\microsoft\directdraw\compatibility\savage[id]
  Oueries value:
  Oueries value:
                                   HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[name]
                                   HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[flags]
  Queries value:
  Oueries value:
                                   HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[id]
  Queries value:
                                   HKLM\software\microsoft\directdraw\compatibility\silentthunder[name]
                                   HKLM\software\microsoft\directdraw\compatibility\silentthunder[flags]
  Oueries value:
                                   \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} in the compatibility \end{tabular} is also compatibility \end{tabular} in the compatibility \en
  Oueries value:
  Oueries value:
                                   HKLM\software\microsoft\directdraw\compatibility\terracide[name]
  Oueries value:
                                   HKLM\software\microsoft\directdraw\compatibility\terracide[flags]
                                   HKLM\software\microsoft\directdraw\compatibility\terracide[id]
  Oueries value:
  Queries value:
                                   HKLM\software\microsoft\directdraw\compatibility\thirddimension[name]
  Oueries value:
                                   HKLM\software\microsoft\directdraw\compatibility\thirddimension[flags]
                                   HKLM\software\microsoft\directdraw\compatibility\thirddimension[id]
  Oueries value:
  Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[name]
  Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[flags]
  Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[id]
  Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[name]
  Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[flags]
  Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[id]
                                   HKLM\software\microsoft\directdraw[modexonly]
  Queries value:
  Queries value:
                                   HKLM\software\microsoft\directdraw[emulationonly]
  Oueries value:
                                   HKLM\software\microsoft\directdraw[showframerate]
  Queries value:
                                   HKLM\software\microsoft\directdraw[enableprintscreen]
  Queries value:
                                   HKLM\software\microsoft\directdraw[forceagpsupport]
  Oueries value:
                                   HKLM\software\microsoft\directdraw[disableagpsupport]
  Queries value:
                                   HKLM\software\microsoft\directdraw[disablemmx]
  Queries value:
                                   HKLM\software\microsoft\directdraw[disableddscapsinddsd]
  Oueries value:
                                   HKLM\software\microsoft\directdraw[disablewidersurfaces]
  Queries value:
                                   HKLM\software\microsoft\directdraw[usenonlocalvidmem]
  Queries value:
                                   HKLM\software\microsoft\directdraw[forcerefreshrate]
  Oueries value:
                                   HKLM\software\microsoft\direct3d[flipnovsync]
                                   HKLM\software\microsoft\directdraw[owndc]
  Queries value:
  Queries value:
                                   HKCR\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserver32[inprocserver32]
                                   HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32[]
  Queries value:
                                   HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}[appid]
  Oueries value:
                                   HKCR\clsid\{a7ee7f34-3bd1-427f-9231-
  Oueries value:
f941e9b7e1fe}\inprocserver32[threadingmodel]
                                   HKCR\dximagetransform.microsoft.shadow\clsid[]
  Queries value:
  Oueries value:
                                   HKCR\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\inprocserver32[inprocserver32]
                                   HKCR\mime\database\content type\image/gif[extension]
  Oueries value:
                                   HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\\\\inprocserver32[]
  Queries value:
                                   HKCR\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}[appid]
  Oueries value:
                                   HKCR\clsid\{e71b4063-3e59-11d2-952a-
  Oueries value:
00c04fa34f05}\inprocserver32[threadingmodel]
                                   HKCR\clsid\{4cb26c03-ff93-11d0-817e-
  Queries value:
0000f87557db}\inprocserver32[inprocserver32]
                                   HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32[]
  Queries value:
                                   HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}[appid]
  Oueries value:
  Oueries value:
                                   HKCR\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserver32[threadingmodel]
                                   HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprocserver32[inprocserver32]
  Oueries value:
                                   HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32[]
                                   HKCR \clsid \ \{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd\} [appid]
  Queries value:
  Queries value:
                                   HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprocserver32[threadingmodel]
                                   HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0\win32[]
  Oueries value:
  Queries value:
                                   HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32[]
  Oueries value:
                                   HKCR\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32[inprocserver32]
                                   HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32[]
  Oueries value:
                                   HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}[appid]
  Queries value:
                                   HKCR\clsid\{275c23e2-3747-11d0-9fea-
  Oueries value:
00aa003f8646}\inprocserver32[threadingmodel]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\nls\codepage[1250]
  Queries value:
                                   HKLM\system\currentcontrolset\control\nls\codepage[1251]
  Oueries value:
                                   HKLM\svstem\currentcontrolset\control\nls\codepage[1253]
  Queries value:
                                   HKLM\system\currentcontrolset\control\nls\codepage[1254]
                                   HKLM\system\currentcontrolset\control\nls\codepage[1255]
  Oueries value:
  Oueries value:
                                   HKLM\system\currentcontrolset\control\nls\codepage[1256]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\nls\codepage[1257]
  Queries value:
                                   HKLM\system\currentcontrolset\control\nls\codepage[1258]
  Oueries value:
                                   HKCR\mime\database\content type\image/png[extension]
  Queries value:
                                   HKLM\system\currentcontrolset\control\nls\codepage[874]
```

HKLM\software\microsoft\directdraw\compatibility\savage[flags]

Oueries value:

Oueries value: HKLM\system\currentcontrolset\control\nls\codepage[932] HKLM\system\currentcontrolset\control\nls\codepage[936] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\codepage[949] HKCR\clsid\{30c3b080-30fb-11d0-b724-Queries value: 00aa006c1a01}\inprocserver32[inprocserver32] Queries value: HKLM\system\currentcontrolset\control\nls\codepage[1361] Oueries value: HKCU\software\microsoft\internet explorer\international\scripts\24[iefontsize] Queries value: HKCU\software\microsoft\internet explorer\international\scripts\24[iefontsizeprivate] Oueries value: HKCU\software\microsoft\internet explorer\international\scripts\24[iepropfontname] Oueries value: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[] Oueries value: HKCU\software\microsoft\internet explorer\international\scripts\24[iefixedfontname] Queries value: HKCU\software\microsoft\internet explorer\international[codepointtofontmap] Queries value: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}[appid] Queries value: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[threadingmodel] Queries value: HKCU\software\microsoft\internet explorer\international\scripts\26[iefontsize] Oueries 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] HKCR\clsid\{6a01fda0-30df-11d0-b724-Oueries value: 00aa006c1a01}\inprocserver32[inprocserver32] Queries value: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32[] HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}[appid] Queries value: HKCR\clsid\{6a01fda0-30df-11d0-b724-Queries value: 00aa006c1a01}\inprocserver32[threadingmodel] HKCR\mime\database\content type\image/bmp\bits[0] Oueries value: Queries value: HKCR\mime\database\content type\image/gif\bits[0] Queries value: HKCR\mime\database\content type\image/jpeg\bits[0] Oueries value: HKCR\mime\database\content type\image/pjpeg\bits[0] HKCR\mime\database\content type\image/png\bits[0] Queries value: Queries value: HKCR\mime\database\content type\image/x-png\bits[0] Oueries value: HKCR\mime\database\content type\image/x-wmf\bits[0] HKCR\mime\database\content type\image/x-png[image filter clsid] Queries value: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-Oueries value: 00a0c913f750}\inprocserver32[inprocserver32] HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[] Oueries value: Queries value: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}[appid] Oueries value: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[threadingmodel] HKLM\software\microsoft\direct3d[disablemmx] Oueries value: Queries value: HKLM\software\microsoft\direct3d[disablex3d] HKLM\software\microsoft\direct3d[fewvertices] Oueries value: Oueries value: HKLM\software\microsoft\direct3d[disablevidmemvbs] Queries value: HKCU\software\microsoft\windows script\settings[jitdebug] HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-Queries value: $77e8f3d1aa80\} \\ category \\ item \\ \{c6debc0a-f2b2-4f17-930e-ca9faff4cd04\}[iconindex]$ Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}[iconindex] Oueries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[iconindex] HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_use_windowedselectcontrol[1af5338669efabe0a9841478396871b1.exe] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_use_windowedselectcontrol[*] Oueries value: HKCU\software\microsoft\internet explorer\new windows[accuserinitonclick] HKCR\shockwaveflash.shockwaveflash\clsid[] Oueries value: Queries value: HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprocserver32[inprocserver32] Queries value: $\label{local-condition} HKCR\clsid\d27cdb6e-ae6d-11cf-96b8-444553540000\\\inprocserver32[]$ HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}[appid] Oueries value: Queries value: HKCR\clsid\{d27cdb6e-ae6d-11cf-96b8-444553540000}\inprocserver32[threadingmodel] HKLM\software\microsoft\directx[glitchinstrumentation] Oueries value: Oueries value: HKLM\hardware\description\system\centralprocessor\0[~mhz] Queries value: $\label{local-eq:hkcr-typelib-def} $$ HKCR \times \frac{d27cdb6b-ae6d-11cf-96b8-444553540000} \ 1.0\ 0 \times 1.0\$ HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32[] Oueries value:

Queries value: folders[local appdata]

Queries value:

Queries value:

Oueries value:

 $\label{thm:linear} \verb|HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]| \\$

 $\label{local-hklm} $HKLM\software\microsoft\internet explorer\default behaviors[userdata] $HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32[]$

HKCU\software\microsoft\windows\currentversion\explorer\user shell

Queries value:

```
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[]
 Oueries value:
 Oueries value:
                         HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
 Oueries value:
HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
 Oueries value:
00c04fb6bfc4}\inprocserver32[inprocserver32]
 Queries value:
                         HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[]
                         HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[appid]
 Oueries value:
 Oueries value:
                         HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[threadingmodel]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2000]
 Queries value:
                         HKLM\software\microsoft\internet explorer\feed discovery[sound]
 Queries value:
                         HKCU\software\microsoft\ftp[use web based ftp]
 Queries value:
                         HKLM\software\microsoft\internet explorer\activex
compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}[compatibility flags]
 Queries value:
                         HKLM\software\microsoft\internet explorer\activex
compatibility\{d27cdb6e-ae6d-11cf-96b8-444553540000}[miscstatus flags]
                         HKCR\clsid\d27cdb6e-ae6d-11cf-96b8-444553540000\miscstatus\1[]
 Queries value:
 Queries value:
                         HKCR\mime\database\content type\application/x-shockwave-flash[extension]
                         HKCR\clsid\{2933bf90-7b36-11d2-b20e-
 Queries value:
00c04f983e60}\inprocserver32[inprocserver32]
                         HKCR\clsid\{2933bf90-7b36-11d2-b20e-00c04f983e60}\inprocserver32[]
 Queries value:
                         \label{locality} $$ HKCR\clsid_{2933bf90-7b36-11d2-b20e-00c04f983e60}[appid] $$
 Queries value:
 Queries value:
                         HKCR\clsid\{2933bf90-7b36-11d2-b20e-
00c04f983e60}\inprocserver32[threadingmodel]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\3[1606]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\userdata[cacherepair]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\userdata[cachepath]
                         \label{lem:hkcu} \verb+KCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
 Oueries value:
settings\5.0\cache\extensible cache\userdata[cacheprefix]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\userdata[cachelimit]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\userdata[cacheoptions]
 Queries value:
                         HKLM\software\microsoft\cryptography\defaults\provider types\type
001[name]
 Oueries value:
                         HKCU\software\microsoft\internet explorer\domstorage\total[]
                         HKCR\clsid\{9ba05972-f6a8-11cf-a442-
 Queries value:
00a0c90a8f39}\inprocserver32[inprocserver32]
                         HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserver32[]
 Queries value:
                         HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}[appid]
 Oueries value:
 Queries value:
                         HKCR\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprocserver32[threadingmodel]
                         HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32[]
 Queries value:
                         HKCR\clsid\{00020424-0000-0000-c000-
 Oueries value:
00000000046}\inprocserver32[inprocserver32]
 Queries value:
                         HKCU\software\microsoft\internet
explorer\services[selectionactivitybuttondisable]
 Oueries value:
                         HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprocserver32[]
 Queries value:
                         HKCU\software\macromedia\flashplayer[flashplayerversion]
                         HKCU\software\microsoft\internet explorer\suggested sites[enabled]
 Oueries value:
 Queries value:
                         HKCR\clsid\{00020424-0000-0000-c000-00000000046}[appid]
 Oueries value:
                         HKLM\system\wpa\pnp[seed]
 Queries value:
                         HKLM\system\setup[osloaderpath]
 Queries value:
                         HKLM\system\setup[systempartition]
                         \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:local_hammon} software \verb|\microsoft| windows \verb|\currentversion| setup[sourcepath] \end{tabular}
 Oueries value:
                         HKCR\clsid\{00020424-0000-0000-c000-
00000000046}\inprocserver32[threadingmodel]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
 Queries value:
\label{thm:local_hammon_hammon} \begin{tabular}{l}{HKLM \software \mbox{$m$icrosoft \windows \current version \setup[service pack cachepath]} \end{tabular}
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
                         HKLM\software\microsoft\windows\currentversion[devicepath]
 Oueries value:
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\setup[loglevel]
                         HKLM\software\microsoft\windows\currentversion\setup[logpath]
 Oueries value:
 Oueries value:
                         HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib[]
 Queries value:
                         HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib[version]
 Queries value:
11e3-9fc7-806d6172696f}[data]
11e3-9fc7-806d6172696f}[generation]
 Queries value:
                         Oueries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [dontshow superhidden]
```

```
Oueries value:
                          HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
                          HKLM\software\microsoft\rpc[udtalignmentpolicy]
 Oueries value:
 Oueries value:
                          Queries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer[forceactive desktop on]]
 Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell]
 Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
                         HKCR\clsid\{00020420-0000-0000-c000-
 Queries value:
00000000046}\inprocserver32[inprocserver32]
 Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
                         \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{tabular} hidden \cite{tabular} \end{tabular}
 Oueries value:
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
                         HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprocserver32[]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
                         HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
                         HKCR\directory[docobject]
 Oueries value:
 Queries value:
                         HKCR\directory[browseinplace]
                          HKCR\clsid\{00020420-0000-0000-c000-00000000046}[appid]
 Oueries value:
 Queries value:
                          HKCR\directory[isshortcut]
 Queries value:
                         HKCR\directory[alwaysshowext]
 Queries value:
                          HKCR\directory[nevershowext]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
                         HKCR\clsid\{00020420-0000-0000-c000-
 Oueries value:
00000000046}\inprocserver32[threadingmodel1
 Queries value:
                         HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32[]
 Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[allowclsidprogidmapping]
 Queries value:
                         HKCR\clsid\{b8da6310-e19b-11d0-933c-
00a0c90dcaa9}\inprocserver32[inprocserver32]
                         HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[docobject]
 Oueries value:
                         HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[browseinplace]
 Oueries value:
                          HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprocserver32[]
 Queries value:
 Queries value:
                          HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[isshortcut]
                          HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000\}[alwaysshowext]
 Oueries value:
                          HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[nevershowext]
 Queries value:
                          HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}[appid]
 Oueries value:
                         HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32[]
 Queries value:
                         HKCR \verb|\clsid| \{ff 393560-c2a 7-11cf-bff 4-
 Oueries value:
444553540000}\inprocserver32[loadwithoutcom]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\shell
extensions\blocked[{ff393560-c2a7-11cf-bff4-444553540000}]
                         HKCU\software\microsoft\windows\currentversion\shell
 Oueries value:
extensions\blocked[{ff393560-c2a7-11cf-bff4-444553540000}]
 Oueries value:
                         HKLM\software\microsoft\windows\currentversion\shell
extensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {e022b1e2-a19e-4b43-8160-7bcecacb3d6e}
0x401]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {e022b1e2-a19e-4b43-8160-7bcecacb3d6e}
0x4011
 Oueries value:
                         HKCR\clsid\{b8da6310-e19b-11d0-933c-
00a0c90dcaa9}\inprocserver32[threadingmodel]
 Oueries value:
                         HKCR\interface\{00020404-0000-0000-c000-00000000046}\proxystubclsid32[]
 Queries value:
                         HKCR\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32[inprocserver32]
 Queries value:
                         HKCR\clsid\{00020421-0000-0000-c000-
```

```
00000000046}\inprocserver32[inprocserver32]
                                                        HKCR\clsid\{00020421-0000-0000-c000-00000000046}\inprocserver32[]
    Oueries value:
                                                        HKCR\clsid\{00020421-0000-0000-c000-00000000046}[appid]
    Oueries value:
                                                        HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[appid]
    Queries value:
                                                        HKCR\clsid\{ff393560-c2a7-11cf-bff4-
    Oueries value:
444553540000}\inprocserver32[threadingmodel]
                                                       HKCR\clsid\{00020421-0000-0000-c000-
    Oueries value:
00000000046}\inprocserver32[threadingmodel]
    Queries value:
                                                        HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042220160423[cacherepair]
                                                       HKCU\software\microsoft\windows\currentversion\internet
    Oueries value:
settings\5.0\cache\extensible cache\mshist012016042220160423[cachepath]
   Queries value:
                                                       HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042220160423[cacheprefix]
    Queries value:
                                                        HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042220160423[cachelimit]
                                                       HKCU\software\microsoft\windows\currentversion\internet
    Oueries value:
settings\5.0\cache\extensible cache\mshist012016042220160423[cacheoptions]
                                                       HKCU\software\microsoft\internet
    Queries value:
explorer\main\windowssearch[enabledscopes]
    Queries value:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[favorites]
    Oueries value:
                                                        HKCR\.url\persistenthandler[]
    Queries value:
                                                        HKLM\software\microsoft\windows search[currentversion]
    Queries value:
                                                        HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsfordisplay]
                                                        HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
08002b30309d}\shellfolder[attributes]
                                                        HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
08002b30309d}\shellfolder[callforattributes]
   Queries value:
08002b30309d}]
    Queries value:
                                                        HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hidefolderverbs]
                                                        HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[localizedstring]
    Queries value:
                                                        HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
    Oueries value:
1757981266-507921405-1957994488-1003[flags]
                                                        HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
    Queries value:
1757981266-507921405-1957994488-1003[state]
                                                       \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the current version \end{tabular} profile list \end{tabular} is the current version \end{tabular} and the current version \
    Queries value:
1757981266-507921405-1957994488-1003[userpreference]
                                                       HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
   Oueries value:
1757981266-507921405-1957994488-1003[centralprofile]
                                                        \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the current version \end{tabular} profile list \end{tabular} is the current version \end{tabular} and the current version \
    Oueries value:
1757981266-507921405-1957994488-1003[profileloadtimelow]
    Queries value:
                                                       HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus profile list \setminus s-1-5-21-1000 + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1)
1757981266-507921405-1957994488-1003[profileloadtimehigh]
                                                       HKCU\software\microsoft\windows\shellnoroam\muicache[langid]
    Oueries value:
    Queries value:
HKCU \ software \ microsoft \ windows \ shell no roam \ muicache [@c:\windows \ system 32\ shell 32.dll, -9216]
                                                        HKLM\software\microsoft\downloadmanager[cacheok]
    Oueries value:
    Queries value:
                                                        HKCU\software\microsoft\internet explorer\domstorage\baidu.com[]
                                                        HKCR\clsid\{f5078f35-c551-11d3-89b9-
    Queries value:
0000f81fe221}\inprocserver32[inprocserver32]
                                                       HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221}\inprocserver32[]
    Queries value:
                                                        HKCR\clsid\{f5078f35-c551-11d3-89b9-0000f81fe221\}[appid]
    Queries value:
    Queries value:
                                                        HKCR\clsid\{f5078f35-c551-11d3-89b9-
0000f81fe221}\inprocserver32[threadingmodel]
                                                        HKCR\shockwaveflash.shockwaveflash.7\clsid[]
    Queries value:
    Queries value:
                                                        HKCR\mime\database\content type\image/x-icon[extension]
                                                       HKCR\clsid\{e569bde7-a8dc-47f3-893f-
    Oueries value:
fd2b31b3eefd}\inprocserver32[inprocserver32]
                                                        HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32[]
    Oueries value:
                                                        HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}[appid]
    Queries value:
                                                        HKCR\clsid\{e569bde7-a8dc-47f3-893f-
    Oueries value:
fd2b31b3eefd}\inprocserver32[threadingmodel]
                                                       HKCR\clsid\{adc6cb82-424c-11d2-952a-
    Queries value:
00c04fa34f05}\inprocserver32[inprocserver32]
                                                        HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}\inprocserver32[]
    Oueries value:
                                                        HKCR\clsid\{adc6cb82-424c-11d2-952a-00c04fa34f05}[appid]
    Queries value:
                                                        HKCR\clsid\{adc6cb82-424c-11d2-952a-
    Oueries value:
00c04fa34f05}\inprocserver32[threadingmodel]
                                                       HKCR\clsid\{0e890f83-5f79-11d1-9043-
    Queries value:
00c04fd9189d}\inprocserver32[inprocserver32]
                                                       HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32[]
    Oueries value:
    Queries value:
                                                        HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}[appid]
                                                        HKCR\clsid\{0e890f83-5f79-11d1-9043-
    Oueries value:
00c04fd9189d}\inprocserver32[threadingmodel]
   Sets/Creates value:
                                                       HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\userdata[cachepath]
                                                        HKCU\software\microsoft\windows\currentversion\internet
    Sets/Creates value:
settings\5.0\cache\extensible cache\userdata[cacheprefix]
```

HKCU\software\microsoft\windows\currentversion\internet Sets/Creates value:

settings\5.0\cache\extensible cache\userdata[cachelimit]

Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\extensible cache\userdata[cacheoptions]

HKCU\software\microsoft\windows\currentversion\internet Sets/Creates value:

settings\5.0\cache\extensible cache\userdata[cacherepair]

Sets/Creates value: HKCU\software\microsoft\internet explorer\domstorage\baidu.com[]

HKCU\software\microsoft\windows\currentversion\internet Sets/Creates value:

settings\5.0\cache\extensible cache\mshist012016042220160423[cachepath]

Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\extensible cache\mshist012016042220160423[cacheprefix]

Sets/Creates value: $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}$

settings\5.0\cache\extensible cache\mshist012016042220160423[cachelimit]

HKCU\software\microsoft\windows\currentversion\internet Sets/Creates value: settings\5.0\cache\extensible cache\mshist012016042220160423[cacheoptions]

Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016042220160423[cacherepair]

Value changes: HKLM\software\microsoft\cryptography\rng[seed]

Value changes: HKCU\software\microsoft\internet explorer\main[disable script debugger]

Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[cache]

Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[cookies]

Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[history]

 $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} in the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu$ Value changes:

settings\zonemap[proxybypass]

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap[intranetname]

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap[uncasintranet]

HKCU\software\microsoft\windows\currentversion\internet Value changes:

settings\zonemap[autodetect]

Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell

folders[common appdata]

HKCU\software\microsoft\windows\currentversion\explorer\shell

HKCU\software\microsoft\windows\currentversion\internet

Value changes:

folders[appdata]

Value changes: settings[proxyenable]

HKCU\software\microsoft\windows\currentversion\internet Value changes:

settings\connections[savedlegacysettings]

HKLM\software\microsoft\directdraw\mostrecentapplication[name] Value changes: HKLM\software\microsoft\directdraw\mostrecentapplication[id] Value changes: Value changes: HKLM\software\microsoft\direct3d\mostrecentapplication[name] HKCU\software\microsoft\windows\currentversion\explorer\shell Value changes:

folders[local appdata]

HKCU\software\microsoft\windows\currentversion\internet Value changes:

settings\5.0\cache\extensible cache\userdata[cachepath]

HKCU\software\microsoft\internet explorer\domstorage\total[] Value changes:

Value changes:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints 2 \ \{f90255c2-6bc4-11e3-9fc7$

806d6172696f}[baseclass]

HKCU\software\microsoft\windows\currentversion\internet Value changes:

settings\5.0\cache\extensible cache\mshist012016042220160423[cachepath]

HKCU\software\microsoft\windows\currentversion\explorer\shell Value changes:

folders[favorites]

HKCU\software\microsoft\internet explorer\main\windowssearch[version] Value changes: Value changes: HKCU\software\microsoft\internet explorer\domstorage\baidu.com[]