Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 236, Task ID: 943

Task ID: 943 Risk Level: 7

Date Processed: 2016-04-28 13:13:28 (UTC)

Processing Time: 61.32 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\f693fea1de37c00fb3925705cbe5722b.exe"

Sample ID: 236 Type: basic Owner: admin

Label: f693fea1de37c00fb3925705cbe5722b

Date Added: 2016-04-28 12:45:14 (UTC)

File Type: PE32:win32:gui File Size: 586008 bytes

MD5: f693fea1de37c00fb3925705cbe5722b

SHA256: 234d3e6a1d9b51d0b5bea97428eb82b86a723d4608d9e34ac484c29c22e5ae6e

Description: None

Pattern Matching Results

2 PE: Nonstandard section

5 Creates process in suspicious location

1 HTTP connection - response code 404 (file not found) [HTTP, GET, POST, web, network, response code]

Creates shortcut on desktop

3 HTTP connection - response code 200 (success) [HTTP, POST, GET, web, network, response code]

🔽 Creates known events: Revenyou [Downware]

3 Long sleep detected

3 Creates a file extension shortcut

3 Connects to local host

4 Packer: NSIS [Nullsoft Scriptable Install System]

Static Events

Anomaly: PE: Contains a virtual section

Anomaly: PE: Contains one or more non-standard sections

Process/Thread Events

Creates process: C:\WINDOWS\Temp\f693fea1de37c00fb3925705cbe5722b.exe

["c:\windows\temp\f693fea1de37c00fb3925705cbe5722b.exe"]

Creates process: C:\DOCUME~1\Admin\LOCALS~1\Temp\DownloadManager.exe

["C:\DOCUME~1\Admin\LOCALS~1\Temp\DownloadManager.exe" /PID=1072 /SUBPID=0 /DISTID=837 /NETWORKID=1 /CID=0 /PRODUCT_ID=752 /SERVER_URL=http://installer.ppdownload.com]

Loads service: RASMAN [C:\WINDOWS\system32\svchost.exe -k netsvcs]
Terminates process: C:\WINDOWS\Temp\f693fea1de37c00fb3925705cbe5722b.exe

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:

ates 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

Creates mutex: \BaseNamedObjects\ZonesCounterMutex

Creates mutex: \BaseNamedObjects\ZoneAttributeCacheCounterMutex
Creates mutex: \BaseNamedObjects\ZonesCacheCounterMutex
Creates mutex: \BaseNamedObjects\ZonesLockedCacheCounterMutex

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

settings!temporary internet files!content.ie5!

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

settings!history!history.ie5!

Creates mutex: \BaseNamedObjects\WininetConnectionMutex
Creates mutex: \BaseNamedObjects\!PrivacIE!SharedMemory!Mutex

Creates mutex: \BaseNamedObjects_!SHMSFTHISTORY!_

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

settings!history!history.ie5!mshist012016042820160429!

Creates mutex: \BaseNamedObjects\MSCTF.Shared.MUTEX.EDH

Creates event: \BaseNamedObjects\userenv: User Profile setup event

Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1} \Creates semaphore: \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57} \Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}

File System Events

```
C:\DOCUME~1\Admin\LOCALS~1\Temp\
 Creates
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsi1.tmp
                         C:\DOCUME~1
 Creates:
                         C:\DOCUME~1\Admin
 Creates:
                         C:\DOCUME~1\Admin\LOCALS~1
 Creates:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp
 Creates:
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\DownloadManager.exe
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsc2.tmp
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsc2.tmp\System.dll
 Creates:
                         C:\Documents and Settings\Admin\Desktop\Continue Man Of Steel
 Creates:
ScreenSaver v2.0.lnk
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\DynamicOfferScreen[1].txt
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\dc[1].js
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\button[1].png
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012016042820160429
 Creates:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012016042820160429\index.dat
                         C:\WINDOWS\Prefetch\F693FEA1DE37C00FB3925705CBE57-10828863.pf
 Opens:
 Opens:
                         C:\Documents and Settings\Admin
                         C:\WINDOWS\Temp\f693fea1de37c00fb3925705cbe5722b.exe
 Opens:
                         C:\WINDOWS\system32\imm32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\shell32.dll
                         C:\WINDOWS\system32\SHELL32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Config
 Opens:
 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\WindowsShell.Manifest
                         C:\WINDOWS\WindowsShell.Config
 Opens:
 Opens:
                         C:\windows\temp\f693fea1de37c00fb3925705cbe5722b.exe.124.Manifest
 Opens:
                         C:\WINDOWS\system32\comctl32.dll
                         C:\WINDOWS\system32\COMCTL32.dll.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\COMCTL32.dll.124.Config
 Opens:
                         C:\WINDOWS\system32\rpcss.dll
 Opens:
                         C:\WINDOWS\system32\MSCTF.dll
 Opens:
                         C:\WINDOWS\system32\shfolder.dll
 Opens:
                         C:\WINDOWS\system32\setupapi.dll
 Opens:
                         C:\
 Opens:
                         C:\Documents and Settings
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsi1.tmp
 Opens:
                         C:\WINDOWS\Temp\b669745d-5bbe-4b73-9f46-723f63e2ed68
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsc2.tmp
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\nsc2.tmp\System.dll}
 Opens:
 Opens:
                         C:\WINDOWS\system32\netapi32.dll
 Opens:
                         C:\Documents and Settings\Admin\My Documents\desktop.ini
 Opens:
                         C:\Documents and Settings\All Users
 Opens:
                         C:\Documents and Settings\All Users\Documents\desktop.ini
 Opens:
                         C:\WINDOWS\system32\clbcatq.dll
 Opens:
                         C:\WINDOWS\system32\comres.dl1
 Opens:
                         C:\WINDOWS\Registration\R00000000007.clb
 Opens:
                         C:\WINDOWS\system32\urlmon.dll
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Config
 Opens:
                         C:\Documents and Settings\Admin\Local Settings
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\DownloadManager.exe}
 Opens:
                         C:\WINDOWS\system32\apphelp.dll
 Opens:
 Opens:
                         C:\WINDOWS\AppPatch\sysmain.sdb
 Opens:
                         C:\WINDOWS\AppPatch\systest.sdb
 Opens:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\DownloadManager.exe.Manifest
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\DownloadManager.exe.Config
 Opens:
                         C:\WINDOWS\Prefetch\DOWNLOADMANAGER.EXE-0331C9C8.pf
 Opens:
                         C:\WINDOWS\system32\winhttp.dll
 Opens:
                         C:\WINDOWS\system32\psapi.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\iphlpapi.dll
                         C:\WINDOWS\system32\ws2_32.dll
 Opens:
                         C:\WINDOWS\system32\ws2help.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Config
 Opens:
                         C:\WINDOWS\svstem32\mswsock.dll
 Opens:
                         C:\WINDOWS\system32\hnetcfg.dll
 Opens:
                         C:\WINDOWS\system32\wshtcpip.dll
 Opens:
                         C:\WINDOWS\system32\dnsapi.dll
 Opens:
                         C:\WINDOWS\system32\drivers\etc\hosts
 Opens:
                         C:\WINDOWS\system32\rsaenh.dll
                         C:\WINDOWS\system32\crypt32.dll
 Opens:
```

```
C:\WINDOWS\system32\rasadhlp.dll
 Opens:
                         C:\WINDOWS\system32\linkinfo.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\ntshrui.dll
 Opens:
                         C:\WINDOWS\system32\atl.dll
 Opens:
                         C:\WINDOWS\system32\ntshrui.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\ntshrui.dll.123.Config
 Opens:
                         C:\Documents and Settings\Admin\Desktop
                         C:\Documents and Settings\Admin\Start Menu\desktop.ini
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\desktop.ini
                         C:\Documents and Settings\All Users\Application Data\desktop.ini
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application Data\desktop.ini
 Opens:
                         C:\WINDOWS
 Opens:
                         C:\Documents and Settings\Admin\My Documents
 Opens:
                         C:\Documents and Settings\Admin\My Documents\My Pictures\Desktop.ini
 Opens:
                         C:\Documents and Settings\All Users\Documents
                         C:\Documents and Settings\All Users\Documents\My Pictures\Desktop.ini
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Documents\My Music\Desktop.ini
 Opens:
                         C:\Documents and Settings\All Users\Documents\My Videos\Desktop.ini
 Opens:
                         C:\WINDOWS\system32\MSCTFIME.IME
 Opens:
                         C:\WINDOWS\system32\ieframe.dll
 Opens:
                         C:\Program Files\Internet Explorer\iexplore.exe
 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\system32\sxs.dll
 Opens:
                         C:\WINDOWS\system32\winlogon.exe
 Opens:
                         C:\WINDOWS\system32\xpsp2res.dll
 Opens:
                         C:\WINDOWS\system32\stdole2.tlb
                         C:\WINDOWS\system32\WININET.dll.123.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\WININET.dll.123.Config
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History
                         C:\Documents and Settings\Admin\Local Settings\History\History.IE5
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\index.dat
                         C:\Documents and Settings\Admin\Cookies
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Cookies\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\index.dat
                         C:\WINDOWS\system32\rasapi32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\rasman.dll
                         C:\WINDOWS\system32\tapi32.dll
 Opens:
 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
                         C:\Documents and Settings\All Users\Application
 Opens:
{\tt Data\Microsoft\Network\Connections\Pbk}
                         C:\WINDOWS\system32\ras
                         C:\AUTOEXEC.BAT
 Opens:
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Microsoft\Network\Connections\Pbk\
 Opens:
                         C:\WINDOWS\system32\sensapi.dll
                         C:\WINDOWS\system32\mlang.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\MLANG.dll.123.Manifest
                         C:\WINDOWS\system32\MLANG.dll.123.Config
 Opens:
                         C:\WINDOWS\system32\MSIMTF.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\msv1_0.dll
 Opens:
                         C:\WINDOWS\system32\mshtml.dll
 Opens:
                         C:\WINDOWS\system32\msls31.dll
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\DynamicOfferScreen[1].txt
                         C:\WINDOWS\system32\jscript.dll
 Opens:
 Opens:
                         C:\WINDOWS\Fonts\times.ttf
 Opens:
                         C:\WINDOWS\Fonts\timesbi.ttf
                         C:\WINDOWS\Fonts\arialbd.ttf
 Opens:
 Opens:
                         C:\WINDOWS\system32\usp10.dll
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\CXCXW1MR\dc[1].js
                         C:\WINDOWS\system32\uxtheme.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\imgutil.dll
 Opens:
                         C:\WINDOWS\system32\pngfilt.dll
                         C:\WINDOWS\system32
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014033120140407
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014033120140407\index.dat
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\MSHist012014041220140413
 Opens:
                         C:\Documents and Settings\Admin\Local
```

```
Settings\History\History.IE5\MSHist012014041220140413\index.dat
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\MSHist012016042820160429
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012016042820160429\index.dat
 Opens:
                         C:\WINDOWS\system32\msimg32.dll
 Opens:
                         C:\WINDOWS\Fonts\wingding.ttf
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\DownloadManager.exe
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsc2.tmp\System.dll
                         C:\Documents and Settings\Admin\Desktop\Continue Man Of Steel
 Writes to:
ScreenSaver v2.0.lnk
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\DynamicOfferScreen[1].txt
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\CXCXW1MR\dc[1].js
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\button[1].png
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012016042820160429\index.dat
                         C:\WINDOWS\Temp\f693fea1de37c00fb3925705cbe5722b.exe
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\My Documents\desktop.ini
                         C:\Documents and Settings\All Users\Documents\desktop.ini
 Reads from:
 Reads from:
                         C:\WINDOWS\Registration\R00000000007.clb
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\DownloadManager.exe
 Reads from:
                         C:\WINDOWS\system32\drivers\etc\hosts
 Reads from:
                         C:\WINDOWS\system32\rsaenh.dll
 Reads from:
                         C:\Documents and Settings\Admin\Start Menu\desktop.ini
 Reads from:
                         C:\Documents and Settings\All Users\Start Menu\desktop.ini
                         C:\Documents and Settings\All Users\Application Data\desktop.ini
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Application Data\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\My Documents\My Pictures\Desktop.ini
                         C:\Documents and Settings\All Users\Documents\My Pictures\Desktop.ini
 Reads from:
 Reads from:
                         C:\Documents and Settings\All Users\Documents\My Music\Desktop.ini
 Reads from:
                         C:\Documents and Settings\All Users\Documents\My Videos\Desktop.ini
 Reads from:
                         C:\WINDOWS\svstem32\ieframe.dll
 Reads from:
                         C:\WINDOWS\system32\stdole2.tlb
 Reads from:
                         C:\AUTOEXEC.BAT
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\dc[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsi1.tmp
 Deletes:
 Deletes:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsc2.tmp
 Deletes:
                         C:\Documents and Settings\Admin\Local Settings\Temp\nsc2.tmp\System.dll
                         C:\Documents and Settings\Admin\Local
 Deletes:
Settings\History\History.IE5\MSHist012014033120140407\index.dat
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014033120140407
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014041220140413\index.dat
                         C:\Documents and Settings\Admin\Local
 Deletes:
Settings\History\History.IE5\MSHist012014041220140413
```

Network Events

-	
DNS query:	installer.ppdownload.com
DNS query:	srv.serverdatasrv.com
DNS query:	static.revenyou.com
DNS query:	stats.g.doubleclick.net
DNS response:	smartinstaller.elasticbeanstalk.com \Rightarrow 184.73.156.182
DNS response:	smartinstaller.elasticbeanstalk.com ⇒ 54.243.188.115
DNS response:	staticrevenyou.outbrowse.netdna-cdn.com ⇒ 198.232.124.224
DNS response:	stats.l.doubleclick.net \Rightarrow 74.125.68.155
DNS response:	stats.l.doubleclick.net \Rightarrow 74.125.68.157
DNS response:	stats.l.doubleclick.net ⇒ 74.125.68.156
DNS response:	stats.l.doubleclick.net ⇒ 74.125.68.154
Connects to:	184.73.156.182:80
Connects to:	127.0.0.1:1050
Connects to:	198.232.124.224:80
Connects to:	74.125.68.155:80
Sends data to:	8.8.8.8:53
Sends data to:	smartinstaller.elasticbeanstalk.com:80 (184.73.156.182)
Sends data to:	127.0.0.1:1050
Sends data to:	stats.l.doubleclick.net:80 (74.125.68.155)
Sends data to:	staticrevenyou.outbrowse.netdna-cdn.com:80 (198.232.124.224)
Receives data from:	0.0.0.0:0
Receives data from:	smartinstaller.elasticbeanstalk.com:80 (184.73.156.182)
Receives data from:	127.0.0.1:1050
Receives data from:	stats.l.doubleclick.net:80 (74.125.68.155)
Receives data from:	staticrevenyou.outbrowse.netdna-cdn.com:80 (198.232.124.224)

Windows Registry Events

```
806d6172696f}\
   Creates key:
                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
   Creates key:
                                                 HKCU\software\microsoft\windows\currentversion\explorer\shell folders
   Creates key:
                                                 HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders
   Creates key:
                                                 HKLM\software\microsoft\windows\currentversion\explorer\shell folders
                                                 HKCR\clsid\{d3388703-5092-487c-8217-11ada1ca68b5}
   Creates key:
   Creates key:
                                                 HKCR\clsid\d3388703-5092-487c-8217-11ada1ca68b5\programmable
                                                 HKCR\clsid\{d3388703-5092-487c-8217-11ada1ca68b5}\localserver32
   Creates key:
   Creates key:
                                                 HKCR\clsid\{d3388703-5092-487c-8217-11ada1ca68b5}\typelib
   Creates key:
                                                 HKCR \ clsid \ \{d3388703-5092-487c-8217-11ada1ca68b5\} \ \ version
   Creates key:
                                                 HKCR\typelib\{dcabb943-792e-44c4-9029-ecbee6265af9}
                                                 HKCR\typelib\{dcabb943-792e-44c4-9029-ecbee6265af9}\1.0
   Creates key:
   Creates key:
                                                 HKCR\typelib\{dcabb943-792e-44c4-9029-ecbee6265af9}\1.0\flags
   Creates key:
                                                 HKCR\typelib\{dcabb943-792e-44c4-9029-ecbee6265af9}\1.0\0
   Creates key:
                                                 HKCR\typelib\{dcabb943-792e-44c4-9029-ecbee6265af9}\1.0\0\win32
   Creates key:
                                                 HKCR\typelib\{dcabb943-792e-44c4-9029-ecbee6265af9}\1.0\helpdir
   Creates key:
                                                 HKCR\interface\{3408ac0d-510e-4808-8f7b-6b70b1f88534}
   Creates key:
                                                 HKCR \verb|\| interface | \{3408ac0d-510e-4808-8f7b-6b70b1f88534\} \verb|\| proxystubclsid| | the statement of the s
   Creates key:
                                                 HKCR \setminus \{3408ac0d-510e-4808-8f7b-6b70b1f88534\} \setminus \{3408ac0d-510e-4806-8f7b-6b70b1f88534\} \setminus \{3408ac0d-510e-4806-8f7b-6b70b1f88534\} \setminus \{3408ac0d-510e-4806-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f7b-6606-8f
   Creates key:
                                                 HKCR\interface\{3408ac0d-510e-4808-8f7b-6b70b1f88534}\typelib
   Creates key:
                                                 \label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ services \+ tcpip \+ parameters
   Creates key:
                                                 HKLM\software\microsoft\windows\currentversion\shell extensions\blocked
   Creates key:
                                                 \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\shell} extensions\label{lem:hkcu} blocked \\
                                                 HKLM\software\microsoft\windows\currentversion\shell extensions\cached
   Creates key:
   Creates key:
                                                 \label{lem:hkcu} \verb+KCU\software\microsoft\windows\currentversion\shell extensions\cached
   Creates key:
                                                 HKCU\software\microsoft\windows\currentversion\internet settings
   Creates kev:
                                                 HKLM\software\microsoft\tracing
   Creates key:
                                                 HKCU\software\microsoft\windows nt\currentversion\winlogon
   Creates key:
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\connections
   Creates key:
                                                 HKCU\software\microsoft\windows nt\currentversion\network\location
awareness
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Creates kev:
settings\p3p\history
   Creates key:
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042820160429
   Creates key:
                                                 HKCU\software\microsoft\internet explorer\main\windowssearch
   Deletes value:
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Deletes value:
settings[proxvoverride]
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Deletes value:
settings[autoconfigurl]
   Opens key:
                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\f693fea1de37c00fb3925705cbe5722b.exe
   Opens key:
                                                 HKLM\system\currentcontrolset\control\terminal server
   Opens key:
                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdi32.dll
                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
options\user32.dll
   Opens key:
                                                 HKLM\system\currentcontrolset\control\session manager
   Opens key:
                                                 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\imm32.dll
                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
options\ntdll.dll
   Opens key:
                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kernel32.dll
                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
options\secur32.dll
   Opens key:
                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll
   Opens key:
                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll
   Opens key:
                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcrt.dll
   Opens key:
                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shlwapi.dll
   Opens kev:
                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shell32.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\ole32.dll
   Opens key:
                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
   Opens key:
                                                 HKLM\system\currentcontrolset\control\error message instrument\
                                                 HKLM\system\currentcontrolset\control\error message instrument
   Opens kev:
   Opens key:
                                                 \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ 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: HKLM\software\microsoft\windows nt\currentversion\winlogon

Opens key: HKLM\

Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance

Opens key: HKLM\system\setup

Opens key: HKCU\

Opens key: HKCU\software\policies\microsoft\control panel\desktop

Opens key: HKCU\control panel\desktop

Opens key:

HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack

Opens key: HKLM\software\microsoft\ole

Opens key: HKCR\interface

Opens key: HKCR\interface\{00020400-0000-c000-0000000000046}

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

options\msctf.dll

Opens key:

HKLM\software\microsoft\ctf\compatibility\f693fea1de37c00fb3925705cbe5722b.exe

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

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

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

options\shfolder.dll

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

Opens key:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} It is a few and in the limit of the limit$

Opens key:

a2d8-08002b30309d}

Opens key: HKCU\software\classes\

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

08002b30309d}\inprocserver32

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

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

Opens key: HKLM\software\microsoft\windows\currentversion\setup\apploglevels
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key: HKLM\software\policies\microsoft\system\dnsclient

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

Opens key: HKLM\software\microsoft\rpc

 $Opens\ key: \\ HKLM\software\microsoft\windows\ nt\currentversion\sim ge \ file\ execution$

Opens key:

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

Opens kev:

 $HKCU \setminus software \\ \mbox{microsoft} \\ \mbox{windows} \\ \mbox{currentversion} \\ \mbox{explorer} \\ \mbox{mountpoints} \\ \mbox{cpc} \\ \mbox{volume} \\ \mbox{f90255c2-6bc4-1000} \\ \mbox{explorer} \\ \mbox{microsoft} \\ \mbox{explorer} \\ \mbox{explorer}$

11e3-9fc7-806d6172696f}\

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\directory

Opens key: HKCR\directory

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

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

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

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

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

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

Opens key: HKCR\folder

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

Opens key: HKCR\folder\clsid

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

options\system.dll

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

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

options\netapi32.dll

HKCU\software\microsoft\windows\currentversion\explorer\fileexts Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.exe

Opens key: HKCU\software\classes\.exe

Opens key: HKCR\.exe

HKCU\software\classes\exefile Opens key:

Opens key: HKCR\exefile

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

HKCR\exefile\curver Opens key: Opens key: HKCR\exefile\

Opens key: HKCU\software\classes\exefile\shellex\iconhandler

HKCR\exefile\shellex\iconhandler Opens key:

Opens key: HKCU\software\classes\systemfileassociations\.exe

Opens key: HKCR\systemfileassociations\.exe

HKCU\software\classes\systemfileassociations\application Opens kev:

Opens key: HKCR\systemfileassociations\application Opens key: HKCU\software\classes\exefile\clsid Opens key: HKCR\exefile\clsid

Opens key: HKCU\software\classes* Opens key: HKCR*

Opens key: HKCU\software\classes*\clsid

Opens key: HKCR*\clsid

Opens key:

HKLM\software\microsoft\windows\currentversion\explorer\shellexecutehooks

HKCU\software\classes\clsid\{aeb6717e-7e19-11d0-97ee-Opens key:

00c04fd91972}\inprocserver32

HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32 Opens key: Opens key: HKLM\software\microsoft\windows\currentversion\policies\associations Opens key: HKCU\software\microsoft\windows\currentversion\policies\associations

HKCU\software\classes\.ade

Opens key:

Opens key: HKCR\.ade HKCU\software\classes\.adp

Opens key: HKCR\.adp Opens key:

Opens key: HKCU\software\classes\.app

Opens key: HKCR\.app HKCU\software\classes\.asp

Opens key:

Opens key: HKCR\.asp

Opens key: HKCU\software\classes\.bas

Opens key: HKCR\.bas

Opens key: HKCU\software\classes\.bat HKCR\.bat Opens kev:

Opens key:

HKCU\software\classes\.cer Opens key: HKCR\.cer

Opens key: HKCU\software\classes\.chm HKCR\.chm

Opens key: Opens key:

HKCU\software\classes\.cmd Opens kev: HKCR\.cmd

Opens key:

HKCU\software\classes\.com Opens key: HKCR\.com HKCU\software\classes\.cpl Opens key:

Opens key: HKCR\.cpl

HKCU\software\classes\.crt Opens key:

HKCR\.crt Opens kev:

Opens key: HKCU\software\classes\.csh

Opens key: HKCR\.csh

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\oleaut32.dll

Opens key: HKLM\software\microsoft\oleaut Opens key: HKLM\software\microsoft\oleaut\userera

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

options\clbcatq.dll

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

HKLM\software\classes Opens key:

Opens key: HKU\ HKCR\clsid Opens kev:

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

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

00c04fb6bfc4}\treatas

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

00c04fb6bfc4}\inprocserver32

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

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

00c04fb6bfc4}\inprocserverx86

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

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

00c04fb6bfc4}\localserver32

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

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

00c04fb6bfc4}\inprochandler32

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

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

00c04fb6bfc4}\inprochandlerx86

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

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

00c04fb6bfc4}\localserver

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

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

options\iertutil.dll

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

options\urlmon.dll

Opens key: HKCU\software\classes\protocols\name-space handler\ Opens key: HKCR\protocols\name-space handler HKCU\software\classes\protocols\name-space handler Opens kev:

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

settings

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

settings

HKCU\software\microsoft\internet Opens kev: 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\

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

Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol $\label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ internet explorer \verb+ main \verb+ feature control+ \\$ Opens key:

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915

HKLM\software\microsoft\internet Opens key:

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

settings\zonemap\ranges\

Opens kev:

HKCU\software\policies\microsoft\windows\currentversion\internet

settings\zonemap\ranges\

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

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

settings\zonemap\

HKCU\software\microsoft\internet Opens key:

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: HKLM\software\policies HKCU\software\policies Opens key:

Opens key: HKCU\software HKLM\software Opens key:

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

settings\zonemap\ranges\

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

settings\zonemap\protocoldefaults\

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

settings\zonemap\domains\

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

settings\zonemap\domains\

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

settings\zonemap\domains\msn.com

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

settings\zonemap\domains\msn.com\related

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination

Opens key: HKLM\software\microsoft\internet

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610

Opens kev: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_http_username_password_disable

Opens key: HKLM\software\microsoft\internet

```
explorer\main\featurecontrol\feature_http_username_password_disable
  Opens key:
                                      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:
                                      HKLM\software\policies\microsoft\internet explorer
  Opens key:
                                      HKLM\software\policies\microsoft\internet explorer\security
                                      HKCU\software\microsoft\windows\currentversion\internet settings\zones\
  Opens key:
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
  Opens key:
                                      \label{lem:hkcu} \mbox{\current} windows \mbox{\current} internet settings \mbox{\current} settings \mbox{\current} and \mbox{\current} settings \mbox{\current} settings
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
                                      \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
  Opens key:
settings\zones\
  Opens key:
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
                                      \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
  Opens key:
settings\zones\0
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
  Opens key:
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
                                      \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
  Opens key:
settings\zones\2
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\2
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\3
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
  Opens key:
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
                                      HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
                                      HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
                                      \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
  Opens key:
settings\lockdown_zones\
  Opens key:
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\0
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\1
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\2
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\2
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\3
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\3
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\4
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\4
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
  Opens key:
                                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
                                      HKCU\software\classes\exefile\shell\open
  Opens kev:
```

HKCR\exefile\shell\open

Opens key:

Opens key: HKCU\software\classes\exefile\shell\open\command

Opens key: HKCR\exefile\shell\open\command

Opens key:

HKCU\software\microsoft\windows\currentversion\policies\explorer\restrictrun HKLM\software\microsoft\windows\currentversion\app Opens kev:

paths\downloadmanager.exe

Opens key: HKCU\software\classes\exefile\shell\open\ddeexec

HKCR\exefile\shell\open\ddeexec Opens key:

Opens key: HKCU\software\classes\applications\downloadmanager.exe

Opens key: HKCR\applications\downloadmanager.exe Opens key: HKCU\software\microsoft\windows\shellnoroam

Opens key: $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ shell no roam\+ muicache$ Opens key: HKCU\software\microsoft\windows\shellnoroam\muicache\

 $\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the local constant \end{tabular} and \end{tabular} in the local constant \end{tabu$ Opens key: Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\apphelp.dll

Opens key: HKLM\system\wpa\tabletpc Opens key: HKLM\system\wpa\mediacenter

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers

HKLM\software\microsoft\windows Opens kev: nt\currentversion\appcompatflags\custom\downloadmanager.exe

Opens key: HKLM\software\policies\microsoft\windows\safer\levelobjects

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths

Opens key:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ paths \ \{dda3f824-d8cb-441b-834d-d8cb-441b$ be2efd2c1a33}

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes Opens key:

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89edd5fbde1328}

Opens key:

b813f72dbb91}

Opens kev:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}

Opens key:

085bcc18a68d}

Opens kev:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2eb91490411bfc}

Opens key:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus urlzones$

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes Opens kev:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones

Opens key:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ \ 65536 \ paths$

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes

Opens key:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 131072 \ paths$

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes

Opens kev:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ \ 262144 \ paths$

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes

Opens kev:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones

 $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus paths$ Opens kev: Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes

Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones

Opens kev:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths

Opens kev:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes

Opens key:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \added \code identifiers \added \code identifiers \added \code identifiers \added \code \$

Opens key:

 $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus paths$

```
Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus has hes
  Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
  Opens kev:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  Opens kev:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus paths
 Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
  Opens kev:
                            HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Opens key:
                            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\downloadmanager.exe
 Opens key:
                            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winhttp.dll
  Opens key:
                            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\psapi.dll
  Opens key:
                            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
                            HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\ws2_32.dll
  Opens key:
                            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iphlpapi.dll
  Opens key:
                            HKLM\software\microsoft\windows\currentversion\internet
settings\winhttp\tracing
                            HKLM\system\currentcontrolset\services\tcpip\linkage
  Opens key:
  Opens key:
                            HKLM\system\currentcontrolset\services\tcpip\parameters\
  Opens key:
                            HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
                            HKLM \verb|\system| current control set \verb|\services| net bt \verb|\parameters|
  Opens key:
  Opens key:
                            \label{lem:hklm} \verb+Kklm\+ software\+ icrosoft\+ ctf\+ compatibility\+ download manager.exe
  Opens key:
                            HKCU\software\classes\clsid
                            HKCU \setminus software \setminus classes \setminus clsid \setminus \{d3388703-5092-487c-8217-11ada1ca68b5\}
  Opens key:
  Opens key:
                            HKCR\clsid\{d3388703-5092-487c-8217-11ada1ca68b5}
  Opens key:
                            HKCU\software\classes\clsid\{d3388703-5092-487c-8217-
11ada1ca68b5}\programmable
                            HKCR\clsid\{d3388703-5092-487c-8217-11ada1ca68b5}\programmable
  Opens key:
                            HKCU\software\classes\clsid\{d3388703-5092-487c-8217-
  Opens kev:
11ada1ca68b5}\localserver32
                            HKCR\clsid\{d3388703-5092-487c-8217-11ada1ca68b5}\localserver32
  Opens kev:
  Opens key:
                            HKCU\software\classes\clsid\{d3388703-5092-487c-8217-
11ada1ca68b5}\typelib
  Opens key:
                            HKCR\clsid\{d3388703-5092-487c-8217-11ada1ca68b5}\typelib
                            HKCU\software\classes\clsid\{d3388703-5092-487c-8217-
  Opens kev:
11ada1ca68b5}\version
                            HKCR\clsid\{d3388703-5092-487c-8217-11ada1ca68b5}\version
  Opens key:
                            HKCU\software\classes\typelib
  Opens key:
  Opens key:
                            HKCR\typelib
  Opens key:
                            HKCU\software\classes\typelib\{dcabb943-792e-44c4-9029-ecbee6265af9}
                            HKCR\typelib\{dcabb943-792e-44c4-9029-ecbee6265af9}
  Opens kev:
  Opens key:
                            HKCU\software\classes\typelib\{dcabb943-792e-44c4-9029-ecbee6265af9}\1.0
                            HKCR\typelib\{dcabb943-792e-44c4-9029-ecbee6265af9}\1.0
  Opens key:
  Opens key:
                            HKCU\software\classes\typelib\{dcabb943-792e-44c4-9029-
ecbee6265af9}\1.0\flags
  Opens key:
                            HKCR\typelib\{dcabb943-792e-44c4-9029-ecbee6265af9}\1.0\flags
  Opens key:
                            HKCU\software\classes\typelib\{dcabb943-792e-44c4-9029-
ecbee6265af9}\1.0\0
                            HKCR\typelib\{dcabb943-792e-44c4-9029-ecbee6265af9}\1.0\0
  Opens key:
                            HKCU\software\classes\typelib\{dcabb943-792e-44c4-9029-
  Opens kev:
ecbee6265af9}\1.0\0\win32
                            HKCR\typelib\{dcabb943-792e-44c4-9029-ecbee6265af9}\1.0\0\win32
  Opens kev:
  Opens key:
                            HKCU\software\classes\typelib\{dcabb943-792e-44c4-9029-
ecbee6265af9}\1.0\helpdir
  Opens key:
                            HKCR \ typelib \ \{dcabb943-792e-44c4-9029-ecbee6265af9\} \ 1.0 \ helpdir
                            HKCU\software\classes\interface
  Opens kev:
                            HKCU \setminus software \setminus classes \setminus interface \setminus \{3408ac0d-510e-4808-8f7b-6b70b1f88534\}
  Opens key:
  Opens key:
                            HKCR\interface\{3408ac0d-510e-4808-8f7b-6b70b1f88534}
  Opens key:
                            HKCU\software\classes\interface\{3408ac0d-510e-4808-8f7b-
6b70b1f88534}\proxystubclsid
```

Opens key:

 $HKCR \verb|\| face \verb|\| \{3408ac0d-510e-4808-8f7b-6b70b1f88534\} \verb|\| proxystubclsid|$

HKCU\software\classes\interface\{3408ac0d-510e-4808-8f7b-Opens kev:

6b70b1f88534}\proxystubclsid32

Opens kev:

Opens key: HKCU\software\classes\interface\{3408ac0d-510e-4808-8f7b-

6b70b1f88534}\typelib

Opens key:

Opens kev:

HKCU\software\classes\http\shell\open\command Opens key: Opens key: HKCR\http\shell\open\command Opens kev: HKLM\software\microsoft\internet explorer HKLM\software\mozilla\mozilla firefox Opens key: Opens kev: HKCU\software\mozilla\mozilla firefox Opens key: HKCU\software\google\update\clients\{8a69d345-d564-463c-aff1a69d9e530f96} Opens key: $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4300-abe3-4300-a$ c7d49d7cecdc} HKLM\software\microsoft\windows\currentversion\internet settings\winhttp Opens kev: Opens key: $\label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet$ settings\connections $\label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet$ Opens key: settings\winhttp\unsafesslapps HKLM\system\currentcontrolset\services\winsock2\parameters Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006 Opens kev: Opens kev: Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5 Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001 Opens key: Opens kev: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mswsock.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\hnetcfg.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\downloadmanager.exe\rpcthreadpoolthrottle HKLM\software\microsoft\rpc\securityservice Opens key: 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: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dnsapi.dll Opens kev: HKLM\svstem\currentcontrolset\services\dnscache\parameters Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rsaenh.dll HKLM\software\policies\microsoft\cryptography Opens kev: Opens key: HKLM\software\microsoft\cryptography Opens key: HKLM\software\microsoft\cryptography\offload Opens key: HKLM\system\currentcontrolset\control\wmi\security Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasadhlp.dll HKCU\software\classes\clsid\{00021401-0000-0000-c000-00000000046} Opens kev: Opens key: HKCR\clsid\{00021401-0000-0000-c000-00000000046}

HKCU\software\classes\clsid\{00021401-0000-0000-c000-Opens key:

000000000046}\treatas

HKCR\clsid\{00021401-0000-0000-c000-00000000046}\treatas Opens key: HKCU\software\classes\clsid\{00021401-0000-0000-c000-Opens key:

00000000046}\inprocserver32

 $\label{locality} HKCR\clsid\{00021401-0000-0000-c000-000000000046}\ \ \ inprocserver 32.$ Opens key:

HKCU\software\classes\clsid\{00021401-0000-0000-c000-Opens key:

000000000046}\inprocserverx86

 $\label{local_hkcr} \mbox{HKCR\clsid\{00021401-0000-0000-c000-000000000046\}\line} \mbox{linprocserverx86}$ Opens key:

HKCU\software\classes\clsid\{00021401-0000-0000-c000-Opens key:

000000000046}\localserver32

 $\label{localserver32} \mbox{HKCR\clsid\{00021401-0000-0000-c000-000000000046\}\localserver32}} \\ \mbox{ } \mbo$ Opens key:

Opens key: HKCU\software\classes\clsid\{00021401-0000-0000-c000-

00000000046}\inprochandler32

Opens key:

HKCU\software\classes\clsid\{00021401-0000-0000-c000-Opens key:

00000000046}\inprochandlerx86

Opens key: HKCR\clsid\{00021401-0000-0000-c000-00000000046}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{00021401-0000-0000-c000-

000000000046}\localserver

Opens key: HKCR\clsid\{00021401-0000-0000-c000-00000000046}\localserver

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

options\linkinfo.dll

Opens key: HKCU\software\classes\network\sharinghandler

Opens key: HKCR\network\sharinghandler

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\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\image file execution

options\ntshrui.dll

Opens key: HKLM\system\currentcontrolset\services\lanmanserver\defaultsecurity Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist

HKCU\software\classes\clsid\{59031a47-3f72-44a7-89c5-Opens key:

5595fe6b30ee}\inprocserver32

HKCR\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\inprocserver32 Opens key:

HKLM\software\\yessearchessoftware\\yessearcheshp Opens key: Opens key: HKLM\software\\walasearchsoftware\\walasearchhp Opens key: HKLM\software\microsoft\windows nt\currentversion\imm

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

options\msctfime.ime

HKCU\software\microsoft\ctf Opens key:

 ${\it HKLM} \\ {\it Software \ } \\ {\it microsoft \ } \\ {\it ctf \ } \\ {\it systems hared} \\$ Opens key:

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

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

Opens key:

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

00c04fd705a2}\inprocserver32

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

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

00c04fd705a2}\inprocserverx86

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

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

00c04fd705a2}\localserver32

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

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

00c04fd705a2}\inprochandler32

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

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

00c04fd705a2}\inprochandlerx86

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

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

Opens kev:

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: HKCU\software\classes\interface\{eab22ac1-30c1-11cf-a7eb-

0000c05bae0b}\typelib

Opens key: Opens key: $\label{local-hkcu} \begin{tabular}{ll} HKCU \software \classes \clsid \a4a1a128-768f-41e0-bf75-e4fddd \cdot \cdo$

Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba} Opens key: HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc-

00aa00404770}\proxystubclsid32

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

Opens key: HKCU\software\classes\interface\{79eac9c4-baf9-11ce-8c8200aa004ba90b}\proxystubclsid32

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

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

00000000046}\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\windows nt\currentversion\image file execution

options\sxs.dll

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

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

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

00a0c90a8f39}\treatas

Opens key: $\label{eq:hkcr} \begin{tabular}{ll} HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\treat as \\ Opens key: \\ HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\treat as \\ \begin{tabular}{ll} HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\treat as \\ \begin{tabular}{ll} HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\treat as \\ \begin{tabular}{ll} HKCU\software\classes\clsid$

00a0c90a8f39}\inprocserver32

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

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}\inprochandler32

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\software\classes\appid\downloadmanager.exe
Opens key: HKCR\appid\downloadmanager.exe

Opens key: HKLM\system\currentcontrol\set\control\lsa

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

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

0080c7f4ee85}\proxystubclsid32

Opens key: HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32 Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-00000000046}

 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-c0000-c0000-c0000-c0000-c0000-c000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c00-c000-c000-c000-c

000000000046}\treatas

00000000046}\inprocserver32

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

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

00000000046}\inprocserverx86

Opens key: HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprocserverx86

000000000046}\localserver32

Opens key: HKCR\clsid\{00020424-0000-0000-c000-0000000046}\localserver32

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

000000000046}\inprochandler32

Opens key: HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprochandler32

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

00000000046}\inprochandlerx86

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

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

00000000046}\localserver

0080c7f4ee85}\forward

0080c7f4ee85}\typelib

 $\label{lem:continuous} Opens key: $$ HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib$$ Opens key: $$ HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}$$$

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

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

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

0000c05bae0b}\1.1\0

0000c05bae0b}\1.1\0\win32

```
HKCR \typelib \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \label{eq:hkcr} $1.1 \o \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0000 c05 bae 0b \eab 22 ac 0-30 c1-11 cf-a7 eb-0
  Opens key:
                                         HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}
  Opens key:
                                         HKCR\typelib\{00020430-0000-0000-c000-00000000046}
  Opens kev:
  Opens key:
                                         HKCU\software\classes\typelib\{00020430-0000-0000-0000-00000000046}\2.0
  Opens key:
                                         HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0
                                         Opens key:
000000000046}\2.0\0
  Opens key:
                                         HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0
                                         HKCU\software\classes\typelib\{00020430-0000-0000-c000-
  Opens key:
00000000046}\2.0\0\win32
  Opens kev:
                                         HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32
                                         HKCU\software\classes\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:
  Opens key:
                                         HKCU\software\classes\interface\{00020400-0000-0000-c000-
000000000046}\proxystubclsid32
                                         Opens key:
                                         HKCU\software\classes\clsid\{00020420-0000-0000-c000-000000000046}
  Opens key:
  Opens key:
                                         HKCR\clsid\{00020420-0000-0000-c000-00000000046}
                                         HKCU\software\classes\clsid\{00020420-0000-0000-c000-
  Opens key:
000000000046}\treatas
                                         HKCR\clsid\{00020420-0000-0000-c000-00000000046}\treatas
  Opens key:
  Opens key:
                                         HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32
                                         HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprocserver32
  Opens key:
  Opens key:
                                         HKCU\software\classes\clsid\{00020420-0000-0000-c000-
00000000046}\inprocserverx86
                                         HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprocserverx86
  Opens key:
  Opens key:
                                         HKCU\software\classes\clsid\{00020420-0000-0000-c000-
00000000046}\localserver32
  Opens key:
                                         HKCR\clsid\{00020420-0000-0000-c000-00000000046}\localserver32
  Opens key:
                                         HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandler32
                                         HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprochandler32
  Opens key:
  Opens key:
                                         HKCU\software\classes\clsid\{00020420-0000-0000-c000-
00000000046}\inprochandlerx86
                                         HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprochandlerx86
  Opens kev:
  Opens key:
                                         HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\localserver
                                         HKCR\clsid\{00020420-0000-0000-c000-00000000046}\localserver
  Opens key:
  Opens key:
                                         HKCU\software\microsoft\internet explorer\main
  Opens key:
                                         HKLM\software\microsoft\internet explorer\main
  Opens key:
                                         HKLM\software\policies\microsoft\internet explorer\main
  Opens key:
                                         HKCU\software\policies\microsoft\internet explorer\main
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{871c5380-42a0-1069-
a2ea-08002b30309d}
  Opens key:
                                         HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32
  Opens key:
```

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

options\xpsp2res.dll

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

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

08002b30309d}\treatas

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

08002b30309d}\inprocserverx86

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

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

08002b30309d}\localserver32

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

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

08002b30309d}\inprochandler32 Opens key:

HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler32

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

08002b30309d}\inprochandlerx86

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandlerx86

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

08002b30309d}\localserver

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

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

settings\5.0\cache

Opens key: $\label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\$

settings\5.0\cache

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

```
settings\5.0\cache\content
                         HKLM\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\content
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
 Opens key:
                          HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
 Opens key:
                          HKLM\software\microsoft\windows\currentversion\internet
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
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\extensible cache\ietld
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\extensible cache\mshist012014033120140407
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
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
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
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
                          HKCU\software\microsoft\internet
 Opens key:
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
                         HKLM\software\microsoft\internet
 Opens key:
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 key:
\verb|explorer\main\featurecontrol\feature\_allow\_long\_international\_file names|\\
                          HKCU\software\microsoft\internet
 Opens key:
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 kev:
explorer\main\featurecontrol\feature disable unicode handle closing callback
                          HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                          HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                          HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature digest no extras in uri
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
 Opens kev:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
                         HKCU\software\microsoft\windows\currentversion\internet settings\wpad
 Opens kev:
 Opens key:
                          HKCU\software\microsoft\internet
```

explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615 HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615 Opens key: HKLM\software\policies\microsoft\internet explorer\browseremulation Opens key: HKCU\software\policies\microsoft\internet explorer\browseremulation Opens key: HKLM\software\microsoft\internet explorer\mediatypeclass HKLM\software\microsoft\windows\currentversion\internet Opens key: settings\accepted documents $\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in constraints and the constraints of the constraints of$ Opens key: HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615 HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\rasman.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rtutils.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\winmm.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\drivers32 Opens key: HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution options\tapi32.dll Opens key: HKLM\software\microsoft\windows\currentversion\telephony Opens key: options\rasapi32.dll Opens key: HKLM\software\microsoft\tracing\rasapi32 HKLM\system\currentcontrolset\control\session manager\environment Opens kev: Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003 HKCU\environment Opens key: Opens key: HKCU\volatile environment Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\sensapi.dll Opens key: HKCU\software\microsoft\internet explorer Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling Opens key: HKCU\software\classes\protocols\name-space handler\http\ Opens key: HKCR\protocols\name-space handler\http Opens key: HKCU\software\classes\protocols\name-space handler*\ HKCR\protocols\name-space handler* Opens key: Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_enable_compat_logging HKLM\software\microsoft\internet Opens key: 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 HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\user agent Opens kev: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent HKLM\software\microsoft\windows\currentversion\internet settings\user Opens key: agent\ua tokens HKLM\software\microsoft\windows\currentversion\internet settings\user Opens key: agent\pre platform Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent\pre platform HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\user agent\pre platform HKLM\software\microsoft\windows\currentversion\internet settings\user Opens key: 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 HKCU\software\microsoft\internet Opens key: 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

HKCU\software\microsoft\internet

HKLM\software\microsoft\internet

HKCU\software\microsoft\windows\currentversion\urlmon settings

explorer\main\featurecontrol\feature_maxconnectionsperserver

explorer\main\featurecontrol\feature_maxconnectionsper1_Oserver

explorer\main\featurecontrol\feature_maxconnectionsper1_Oserver

Opens key:

Opens key:

Opens key:

Opens key:

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 kev: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_include_port_in_spn_kb908209

HKLM\software\microsoft\internet Opens key:

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\mlang.dll

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_disable_legacy_compression HKLM\software\microsoft\internet Opens key: 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\classes\clsid\{d3388703-5092-487c-8217-

11ada1ca68b5}\treatas

Opens key: HKCR\clsid\{d3388703-5092-487c-8217-11ada1ca68b5}\treatas Opens key: HKCU\software\classes\clsid\{d3388703-5092-487c-8217-

11ada1ca68b5}\inprocserver32

HKCR\clsid\{d3388703-5092-487c-8217-11ada1ca68b5}\inprocserver32 Opens kev:

Opens key: HKCU\software\classes\clsid\{d3388703-5092-487c-8217-

11ada1ca68b5}\inprocserverx86

HKCR\clsid\{d3388703-5092-487c-8217-11ada1ca68b5}\inprocserverx86 Opens key:

Opens key: HKCU\software\classes\clsid\{d3388703-5092-487c-8217-

11ada1ca68b5}\inprochandler32

HKCR\clsid\{d3388703-5092-487c-8217-11ada1ca68b5}\inprochandler32 Opens kev:

Opens key: HKCU\software\classes\clsid\{d3388703-5092-487c-8217-

11ada1ca68b5}\inprochandlerx86

HKCR\clsid\{d3388703-5092-487c-8217-11ada1ca68b5}\inprochandlerx86 Opens key:

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

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

options\msv1_0.dll

HKCU\software\classes\mime\database\content type\text/html; charset=utf-Opens key:

Opens key: HKCR\mime\database\content type\text/html; charset=utf-8 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \mime \database \content type \text/html \end{tabular}$ Opens key:

Opens key: HKCR\mime\database\content type\text/html

Opens key: HKCU\software\classes\protocols\filter\text/html; charset=utf-8

HKCR\protocols\filter\text/html; charset=utf-8 Opens key: Opens key: HKCU\software\classes\protocols\filter\text/html

HKCR\protocols\filter\text/html Opens kev: HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_mime_sniffing Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_mime_sniffing

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

HKLM\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_feeds

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

 $HKCU \setminus software \setminus classes \setminus clsid \setminus \{25336920-03f9-11cf-8fd0-00aa00686f13\}$ Opens key:

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

00aa00686f13}\treatas

Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-

00aa00686f13}\inprocserver32

Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32

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

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

00aa00686f13}\inprochandler32

HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler32 Opens kev:

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 kev:

00aa00686f13}\localserver

```
HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\localserver
 Opens key:
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
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
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_aria_support
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_aria_support
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_private_font_setting
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_private_font_setting
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_css_show_hide_events
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_css_show_hide_events
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_display_node_advise_kb833311
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_expanduri_bypass
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_expanduri_bypass
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_enforce_bstr
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_object_caching
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
                         HKLM\software\microsoft\internet
 Opens kev:
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
                         \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ app\ paths\+ outlook\+ . exe
 Opens key:
 Opens key:
                         HKLM\software\microsoft\internet explorer\application compatibility
 Opens key:
                         HKLM\software\policies\microsoft\internet explorer\domstorage
 Opens key:
                         HKCU\software\policies\microsoft\internet explorer\domstorage
 Opens key:
                         HKCU\software\microsoft\internet explorer\domstorage
                         HKLM\software\microsoft\internet explorer\domstorage
 Opens kev:
                         HKLM\software\policies\microsoft\internet explorer\safety\privacie
 Opens key:
 Opens key:
                         HKCU\software\policies\microsoft\internet explorer\safety\privacie
 Opens key:
                         HKCU\software\microsoft\internet explorer\safety\privacie
 Opens kev:
                         HKLM\software\microsoft\internet explorer\safety\privacie
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_manage_script_circular_refs
```

HKLM\software\microsoft\internet

Opens key:

explorer\main\featurecontrol\feature_manage_script_circular_refs HKCU\software\microsoft\internet Opens key: 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 key: detection HKLM\software\microsoft\internet explorer\security\adv addrbar spoof Opens key: detection Opens kev: HKCU\software\classes\protocols\name-space handler\about\ Opens key: HKCR\protocols\name-space handler\about Opens key: HKCU\software\classes\protocols\handler\about Opens key: HKCR\protocols\handler\about HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b} Opens key: Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b} Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas Opens key: $HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas$ Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32 $HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32$ Opens key: Opens kev: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86 Opens key: $HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\ \ in procserver x 86$ HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\localserver32 HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver32 Opens key: Opens kev: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32 Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32 HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\inprochandlerx86 Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86 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 Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\zones\3 Opens key: HKLM\software\policies\microsoft\internet explorer\zoom HKCU\software\policies\microsoft\internet explorer\zoom Opens key: Opens key: HKCU\software\microsoft\internet explorer\zoom Opens key: HKLM\software\microsoft\internet explorer\zoom HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_weboc_document_zoom HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_weboc_document_zoom Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\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: Opens key: HKLM\software\policies\microsoft\internet explorer\international\scripts Opens key: HKCU\software\microsoft\internet explorer\international\scripts Opens key: HKLM\software\microsoft\internet explorer\international\scripts Opens key: HKLM\software\policies\microsoft\internet explorer\settings Opens key: HKCU\software\microsoft\internet explorer\settings Opens key: HKLM\software\microsoft\internet explorer\settings Opens key: HKCU\software\microsoft\internet explorer\styles Opens key: HKCU\software\microsoft\windows\currentversion\policies\activedesktop HKCU\software\microsoft\windows\currentversion\policies Opens key: Opens key: HKCU\software\microsoft\internet explorer\pagesetup Opens key: HKCU\software\microsoft\internet explorer\menuext HKCU\software\microsoft\internet explorer\menuext\%s Opens key: Opens key: HKLM\system\currentcontrolset\control\nls\codepage Opens key: HKCU\software\microsoft\internet explorer\international\scripts\3 HKLM\software\microsoft\internet explorer\version vector Opens key: Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature zone elevation HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_zone_elevation Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_xssfilter

explorer\main\reaturecontrol\reature_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: HKCU\software\microsoft\internet explorer\dxtrans
Opens key: HKCU\software\microsoft\internet explorer\dxtrans
Opens key: HKCU\software\microsoft\internet explorer\dxtrans

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_sslux

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_sslux

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

settings\

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

settings\zonemap\

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

settings\zonemap\

Opens key: HKLM\software\policies\microsoft\internet explorer\restrictions HKCU\software\policies\microsoft\internet explorer\restrictions Opens key: Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}

HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc} Opens key: Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-

f4ceaaf59cfc}\treatas

Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\treatas Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{50d5107a - d278 - 4871 - 8989 - d278 - d$

f4ceaaf59cfc}\inprocserver32

HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32 Opens key:

HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-Opens kev:

f4ceaaf59cfc}\inprocserverx86

Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-

f4ceaaf59cfc}\localserver32

Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\localserver32

HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-Opens kev:

f4ceaaf59cfc}\inprochandler32

Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandler32

HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-Opens key:

f4ceaaf59cfc}\inprochandlerx86

Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandlerx86

HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-Opens key:

f4ceaaf59cfc}\localserver

HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\localserver Opens kev:

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

options\msimtf.dll

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

 $HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8$ Opens key:

c9633f71be64}\languageprofile

HKCU\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-Opens kev:

c9633f71be64}\languageprofile

 $HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8$ Opens key:

c9633f71be64}\languageprofile\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\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53} Opens kev:

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

Opens key:

HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\treatas HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-Opens key: 431b3828ba53}\inprocserver32

Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32

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

431b3828ba53}\inprocserverx86

HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserverx86 Opens key:

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

431b3828ba53}\localserver32

Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver32

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

431b3828ba53}\inprochandler32

HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandler32 Opens key:

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

431b3828ba53}\inprochandlerx86

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

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

431b3828ba53}\localserver

 $\label{localserver} $HKCR\clsid{3ce74de4-53d3-4d74-8b83-431b3828ba53} \setminus localserver $$ (a) $ (a) $ (b) $ (b) $ (b) $ (c) $ ($ Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7} Opens key:

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

869523e2d6c7}\treatas

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

869523e2d6c7}\inprocserver32

HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserver32 Opens kev:

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

869523e2d6c7}\inprocserverx86

HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserverx86 Opens key:

Opens key:

```
869523e2d6c7}\localserver32
                                                                                               HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\localserver32
      Opens key:
      Opens key:
                                                                                                HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprochandler32
      Opens kev:
                                                                                                HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandler32
      Opens key:
                                                                                                869523e2d6c7}\inprochandlerx86
                                                                                               HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandlerx86
      Opens key:
      Opens key:
                                                                                                869523e2d6c7}\localserver
                                                                                               HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\localserver
      Opens key:
      Opens key:
                                                                                                HKLM\software\microsoft\ctf\tip\
      Opens key:
                                                                                                c9633f71be64}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
      Opens key:
                                                                                                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
      Opens kev:
                                                                                                HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
e988c088ec82}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
     Opens key:
                                                                                                HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
00c04fc324a1}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
      Opens key:
                                                                                                HKLM\software\microsoft\ctf\tip\f89e9e58-bd2f-4008-9ac2-
Of816c09f4ee}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
                                                                                                HKCU\software\microsoft\ctf\langbaraddin\
      Opens kev:
      Opens key:
                                                                                                HKLM\software\microsoft\ctf\langbaraddin\
      Opens key:
                                                                                                HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
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}
     Opens key:
                                                                                                HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
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:
Of816c09f4ee}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
                                                                                                HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
      Opens key:
c9633f71be64}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
                                                                                                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
     Opens kev:
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
                                                                                                HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
      Opens key:
c9633f71be64}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
      Opens key:
                                                                                                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
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
                                                                                                HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
     Opens kev:
c9633f71be64\\ \\ \\ category\\ \\ \\ item\\ \\ \\ c6debc0a-f2b2-4f17-930e-ca9faff4cd04\\ \\ \\ \\
                                                                                                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
      Opens kev:
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
      Opens key:
                                                                                                HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
c9633f71be64}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                                                                                                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
     Opens kev:
77e8f3d1aa80}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                                                                                                HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
      Opens key:
e988c088ec82}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
      Opens key:
                                                                                                HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-14d}
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\policies\microsoft\internet explorer\control panel
      Opens key:
                                                                                                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
      Opens key:
                                                                                                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
                                                                                               HKCU \setminus software \setminus classes \setminus clsid \setminus \{f414c260-6ac0-11cf-b6d1-00aa00bbbb58\}
      Opens key:
      Opens key:
                                                                                                HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
      Opens key:
                                                                                                HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\treatas
      Opens key:
                                                                                                HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\treatas
      Opens key:
                                                                                                HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\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
      Opens key:
                                                                                                HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\localserver32
                                                                                                HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
      Opens kev:
00aa00bbbb58}\inprochandler32
                                                                                                HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}\inprochandler32
      Opens kev:
                                                                                                HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
      Opens key:
00aa00bbbb58}\inprochandlerx86
                                                                                                HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\ \ \ in prochandler x 86
```

HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-

Opens key:

Opens kev:

00aa00bbbb58}\localserver

 $HKCR \ clsid \ \{f414c260-6ac0-11cf-b6d1-00aa00bbbb58\} \ localserver$ Opens key:

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

options\jscript.dll

HKLM\software\microsoft\windows script\features Opens key:

Opens kev: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547 Opens key: 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\microsoft\internet

explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert

HKLM\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert

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_scripturl_mitigation Opens key: HKLM\software\microsoft\internet

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

HKLM\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_block_lmz_img

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

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

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

options\usp10.dll

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561

Opens key: HKCU\software\microsoft\internet explorer\feed discovery Opens key: HKLM\software\microsoft\internet explorer\feed discovery

Opens key: HKCU\software\microsoft\ftp

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

options\uxtheme.dll

 $\label{thm:linear} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\thememanager}} \\$ Opens key:

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation

Opens key: HKCU\software\microsoft\internet $\verb|explorer\main\featurecontrol\feature_block_lmz_script| \\$ HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_block_lmz_script

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

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

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

00aa006c1a01}\treatas

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

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

00aa006c1a01}\localserver32

Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver32

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

00aa006c1a01}\inprochandler32

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

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

HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver Opens kev: Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}

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

00aa006c1a01}\treatas

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

00aa006c1a01}\inprocserver32

 $HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\tinprocserver32$ Opens key:

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

00aa006c1a01}\inprocserverx86

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

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

00aa006c1a01}\localserver32

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

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

00aa006c1a01}\inprochandler32

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

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

00aa006c1a01}\inprochandlerx86

Opens key: $HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01\}\ \ inprochandlerx86$

Opens key:

00aa006c1a01}\localserver

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

HKCU\software\classes\mime\database\content type Opens kev:

Opens key: HKCR\mime\database\content type

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

Opens key: HKCR\mime\database\content type\image/bmp\bits

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

Opens key: HKCR\mime\database\content type\image/gif\bits

Opens kev: HKCU\software\classes\mime\database\content type\image/jpeg\bits

Opens key: HKCR\mime\database\content type\image/jpeg\bits

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

Opens key: ${\tt HKCR\mbox{\tt mime}\database\content\ type\limage/pjpeg\bits}$

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

Opens key:

HKCU\software\classes\mime\database\content type\image/tiff\bits

Opens key: HKCR\mime\database\content type\image/tiff\bits

Opens key: HKCU\software\classes\mime\database\content type\image/x-icon\bits

Opens key: HKCR\mime\database\content type\image/x-icon\bits

Opens key: $\label{local-loc$

Opens key: HKCR\mime\database\content type\image/x-jg\bits

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \mbox{$\mbox{mime} \database \content type \label{lem:hkcu} } type \mbox{$\mbox{\mbox Opens key:

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

Opens key: HKCU\software\classes\mime\database\content type\image/x-wmf\bits

Opens key: HKCR\mime\database\content type\image/x-wmf\bits

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

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

 $HKCU \setminus software \setminus classes \setminus clsid \setminus \{a3ccedf7-2de2-11d0-86f4-00a0c913f750\}$ 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

Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32

HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-Opens kev:

00a0c913f750}\inprocserverx86

HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserverx86 Opens key:

HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-Opens key:

00a0c913f750}\localserver32

HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-

00a0c913f750}\inprochandler32

 $HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\$ Opens key:

HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-Opens key:

00a0c913f750}\inprochandlerx86

Opens key:

Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-

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: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_binary_caller_service_provider

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_binary_caller_service_provider HKCU\software\classes\typelib\{dcabb943-792e-44c4-9029-Opens kev:

ecbee6265af9}\1.0\409

Opens key: HKCR\typelib\{dcabb943-792e-44c4-9029-ecbee6265af9}\1.0\409 Opens key: HKCU\software\classes\typelib\{dcabb943-792e-44c4-9029-

ecbee6265af9}\1.0\9

settings\p3p\history\serverdatasrv.com

Opens key: HKCR\typelib\{dcabb943-792e-44c4-9029-ecbee6265af9}\1.0\9 HKCU\software\microsoft\internet explorer\ietld\lowmic Opens kev: $\label{lem:hkcu} \verb+KKCU \software \verb+microsoft + windows \verb+current version \verb+\internet+ \\$ Opens key:

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

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

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

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

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

explorer\infodelivery\restrictions

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

explorer\infodelivery\restrictions

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

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

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

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

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

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

444553540000}\shellex\iconhandler

HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\shellex\iconhandler Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff39560 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff3960 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff3960 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff3960 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff3960 - c2a7 - 11cf - bff4 - 444553540000\} \setminus clsid \setminus \{ff3960 - c2a7 - 11cf - bff4 - 4445535400000\} \setminus clsid \setminus \{ff3960 - c2a7 - 11cf - bff4 - 4445535400000\} \setminus clsid \setminus \{ff3960 - c2a7 - 11cf - bff4 - 4445535400000\} \setminus clsid \setminus \{ff3960 - c2a7 - 11cf - bff4 - 4445535400000\} \setminus clsid \setminus \{ff3960 - c2a7 - 11cf - bff4 - 4445535400000\} \setminus clsid \setminus \{ff3960 - c2a7 -$ Opens key:

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

444553540000}\inprocserver32

Opens key: $HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\tinprocserver32$

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

444553540000}\treatas

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

444553540000}\inprocserverx86

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

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

444553540000}\localserver32

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

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

444553540000}\inprochandler32

Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandler32

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

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

Opens key:

 $HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ objects \ \{ff393560-c2a7-11cf-mail \ constant \ co$

bff4-444553540000}

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

settings\5.0\cache\extensible cache\mshist012016042820160429

Opens key: HKCU\software\microsoft\internet explorer\main\windowssearch HKLM\software\policies\microsoft\internet explorer\feeds Opens key:

Opens key: HKCU\software\microsoft\internet explorer\feeds Opens key: HKLM\software\microsoft\internet explorer\feeds $\label{lem:hkcu} \verb+KKCU \software \classes \. url \persistenthandler$ Opens key:

Opens key: HKCR\.url\persistenthandler

HKLM\software\policies\microsoft\internet explorer\main\windowssearch Opens kev:

HKLM\software\microsoft\windows search Opens key:

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

08002b30309d}\shellfolder

Opens key:

Opens key: $HKCU \ software \ microsoft \ windows \ current version \ explorer \ clsid \ \{20d04fe0-derivation\} \ derivative \ deriva$

3aea-1069-a2d8-08002b30309d}

HKCU\software\microsoft\windows\currentversion\policies\nonenum Opens key: Opens key: HKLM\software\microsoft\windows\currentversion\policies\nonenum

Opens key:

3aea-1069-a2d8-08002b30309d}\shellfolder

Opens key:

3aea-1069-a2d8-08002b30309d}\shellfolder

 $HKCU \setminus software \setminus classes \setminus clsid \setminus \{20d04fe0-3aea-1069-a2d8-08002b30309d\}$ Opens key:

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

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

options\msimg32.dll

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

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

00aa003f8646}\treatas

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

00aa003f8646}\inprocserver32

 $HKCR \ clsid \ \{275c23e2-3747-11d0-9fea-00aa003f8646\} \ \ inprocserver 32$ Opens key:

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

00aa003f8646}\inprocserverx86

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

00aa003f8646}\localserver32

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

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

00aa003f8646}\inprochandler32

Opens key: $HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\tinprochandler 32$

 $HKCU \setminus software \setminus classes \setminus clsid \setminus \{275c23e2-3747-11d0-9fea-4864\} + \{275c23e2-3746\} + \{275c23e2-3764\} + \{275c23e2-3766\} + \{275c23e2-376$ Opens key:

00aa003f8646}\inprochandlerx86

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

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

00aa003f8646}\localserver

 $\label{localserver} $HKCR\clsid\\{275c23e2-3747-11d0-9fea-00aa003f8646}\\\localserver$ Opens key: Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat] Oueries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]

Oueries value:

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

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

nt\currentversion\compatibility32[f693fea1de37c00fb3925705cbe5722b]

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

compatibility[f693fea1de37c00fb3925705cbe5722b]

HKLM\software\microsoft\windows nt\currentversion\windows[appinit dlls] Oueries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]

Queries value: HKLM\system\setup[systemsetupinprogress] Oueries value: HKCU\control panel\desktop[multiuilanguageid] Queries value: HKCU\control panel\desktop[smoothscroll]

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]

HKLM\system\currentcontrolset\control\session Queries value:

manager[criticalsectiontimeout]

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

Queries value: HKCR\interface[interfacehelperdisableall]

Queries value: HKCR\interface[interfacehelperdisableallforole32] Oueries value: HKCR\interface[interfacehelperdisabletypelib] HKCR\interface\{00020400-0000-0000-c000-Queries value:

00000000046}[interfacehelperdisableall]

HKCR\interface\{00020400-0000-0000-c000-Queries value:

00000000046}[interfacehelperdisableallforole32]

HKLM\software\microsoft\ctf\systemshared[cuas] Queries value: HKCU\keyboard layout\toggle[language hotkey] Oueries value:

HKCU\keyboard layout\toggle[hotkey] Queries value: HKCU\keyboard layout\toggle[layout hotkey] Oueries value: Oueries value: HKLM\software\microsoft\ctf[enableanchorcontext] Queries 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]

HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups] Oueries value:

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

Oueries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders] HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[]

Oueries value: Oueries value: HKLM\system\wpa\pnp[seed] Queries value: HKLM\system\setup[osloaderpath] Queries value: HKLM\system\setup[systempartition]

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

Queries value:

HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]

Oueries value:

 $HKLM \verb|\software\m| icrosoft \verb|\windows\currentversion\setup[service pack cache path]|$

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

Queries value: HKLM\software\microsoft\windows\currentversion[devicepath] Oueries value: HKLM\software\microsoft\windows\currentversion\setup[loglevel] HKLM\software\microsoft\windows\currentversion\setup[logpath] Queries value: Oueries value:

 $\label{thm:local_computername} \label{thm:local_computername} HKLM \end{constraints} \begin{center} HKLM \end{constraints} \begin{center} Active computername \end{computername} \begin{center} Active computername \end{center} \begin{center} Active computername \end{cen$ HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] Oueries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]

Oueries value: HKLM\software\microsoft\rpc[maxrpcsize]

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-11e3-9fc7-806d6172696f}[data]

11e3-9fc7-806d6172696f}[generation]

Queries value: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-

409d6c4515e9}[drivemask]

Queries value:

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

HKCU\software\microsoft\windows\currentversion\explorer[shellstate] Oueries value:

Oueries value:

Oueries value:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer[noactive desktop]$

Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu] $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus advanced [hidden]$ Oueries value: Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn] HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview] $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \current version \explorer \advanced [filter] \end{tabular}$ Oueries value: Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling] HKCR\directory[docobject] Queries value: Queries value: HKCR\directory[browseinplace] Oueries value: HKCR\directory[isshortcut] HKCR\directory[alwaysshowext] Queries value: Queries value: HKCR\directory[nevershowext] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps] HKLM\software\microsoft\windows\currentversion\explorer[maximizeapps] Queries value: Queries value: $\label{thm:local_thm:local_thm} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| policies \verb|\explorer[allowfileclsid]| unctions] \end{tabular}$ HKCR\.exe[] Queries value: HKCR\exefile[docobject] Oueries value: Queries value: HKCR\exefile[browseinplace] HKCR\exefile[isshortcut] Oueries value: Queries value: HKCR\exefile[alwaysshowext] Queries value: HKCR\exefile[nevershowext] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[personal] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache] HKLM\software\microsoft\windows\currentversion\explorer\user shell Oueries value: folders[common documents] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[desktop] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[common desktop] HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32[] Oueries value: Queries value: HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32[loadwithoutcom] Queries value: HKCR\.asp[] Oueries value: HKCR\.bat[] Queries value: HKCR\.cer[] Queries value: HKCR\.chm[] HKCR\.cmd[] Oueries value: HKCR\.com[] Oueries value: Queries value: HKCR\.cpl[] Oueries value: HKCR\.crt[] Queries value: HKLM\software\microsoft\com3[com+enabled] Oueries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess] Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject] HKLM\software\microsoft\com3[regdbversion] Oueries value: Oueries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[inprocserver32] Queries value: $HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\nprocserver32[]$ HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[appid] Oueries value: Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[threadingmodel] HKLM\software\microsoft\windows\currentversion\internet

settings[disableimprovedzonecheck] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[f693fea1de37c00fb3925705cbe5722b.exe] Queries value: HKLM\software\microsoft\internet

Oueries value:

```
explorer\main\featurecontrol\feature_protocol_lockdown[*]
                                                 HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
   Oueries value:
   Queries value:
                                                  HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
   Queries value:
                                                 \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
settings[createuricachesize]
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[enablepunycode]
   Queries value:
                                                  HKLM\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
   Queries value:
                                                  HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\zones\1[flags]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[flags]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\zones\3[flags]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\zones\4[flags]
                                                  HKCU\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[f693fea1de37c00fb3925705cbe5722b.exe]
                                                 HKCU\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
                                                 HKLM\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[f693fea1de37c00fb3925705cbe5722b.exe]
                                                 HKLM\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
   Queries value:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
                                                 HKLM\software\microsoft\windows\currentversion\internet
   Queries value:
settings[specialfolderscachesize]
                                                 \label{thm:local_equation} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell} \\
   Queries value:
folders[cache]
   Queries value:
                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\zones\0[1806]
                                                  HKCR\exefile\shell\open\command[]
   Queries value:
                                                  HKCR\exefile\shell\open\command[command]
   Oueries value:
   Oueries value:
                                                  HKCU\software\microsoft\windows\shellnoroam\muicache[langid]
HKCU \ software \ microsoft \ windows \ shell no roam \ muicache \ [c:\ docume-1\ admin\ locals-1\ temp\ download \ manager.exe]
   Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ (explorer \ file association \ [cutlist]) \ description \ descriptio
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[inheritconsolehandles]
   Oueries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [restrict run]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[disallowrun]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[norunasinstallprompt]
   Oueries value:
                                                 HKLM\system\currentcontrolset\control\session
manager\appcompatibility[disableappcompat]
   Oueries value:
                                                 HKLM\system\wpa\mediacenter[installed]
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [authenticode enabled]
   Oueries value:
                                                 HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}[itemdata]
be2efd2c1a33}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemdata]
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[hashalg]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemsize]
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{349d35ab-37b5-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-46666
edd5fbde1328}[saferflags]
   Queries value:
b813f72dbb91}[itemdata]
```

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[hashalg]

Queries value:

Oueries value:

Queries value:

Oueries value:

 $HKLM \software \policies \microsoft \windows \safer \code identifiers \one \noise \n$

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-b91490411bfc\} [item data]$

Queries value:

Queries value:

Queries value:

Queries value:

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

Queries value

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

 $\label{thm:condition} Queries \ value: \\ HKCU \ software \ microsoft \ windows \ current version \ (explorer \ shell) \\$

folders[cache]
Oueries value:

 $HKLM \verb|\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]|$

Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[downloadmanager]

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

compatibility[downloadmanager]

Oueries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_protocol_lockdown[downloadmanager.exe]

Queries value: HKCR\interface\{3408ac0d-510e-4808-8f7b-6b70b1f88534}[]

Queries value: HKCR\interface\{3408ac0d-510e-4808-8f7b-6b70b1f88534}\typelib[]
Queries value: HKCR\interface\{3408ac0d-510e-4808-8f7b-6b70b1f88534}\typelib[version]

Queries value: HKCR\http\shell\open\command[]

Queries value: HKLM\software\microsoft\internet explorer[version]
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]

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

Queries value:

 $HKLM \ system \ current controls et \ services \ trip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [lease obtained time]$

Queries value:

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

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \true \parameters \end{16325b0b-4636-4303-abe3-c7d49d7cecdc} \end{16325b0b-4636-abe3-c7d49d7cecdc} \end{16325b0$

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

settings[sharecredswithwinhttp]

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

settings\connections[winhttpsettings]

Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [winsock_registry_version]$

Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9[serial access num]

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]

Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries \ 000000000001 \ [packed catalog item] \ Queries \ value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000002[packedcatalogitem]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
Queries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ catalog_entries \ 0000000000005 \ [packed catalog item] \ Queries \ value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem] Queries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ catalog_entries \ 0000000000007 \ [packed catalog item] \\ Queries \ value:$

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries \ 0000000000008 \ [packed catalog item] \\ Queries \ value:$

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

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 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\000000000001[displaystring]
Oueries 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]
Queries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
Oueries 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\000000000002[displaystring]
Oueries value:

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 00000000000002 [providerid] \ Oueries \ value:$

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

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

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 00000000000002 \ [enabled] \ Oueries \ value:$

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

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

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

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

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

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

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

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \names pace_catalog 5 \catalog_entries \names \pace_catalog 5 \catalog_entries \pace_catalog 5 \catalog 6 \catalog 6 \catalog 6 \catalog 6 \catalog 6 \c$

```
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ (version) \ and \ services \ (version) \ and \ (
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_\catalog_entries\00000000003[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
  Oueries value:
                                     HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
  Oueries value:
                                     HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Queries value:
                                     HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
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]
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]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
  Oueries value:
                                     HKLM\svstem\currentcontrolset\services\dnscache\parameters[useedns]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [queryipm atching]
  Queries value:
                                     HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
  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]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
  Oueries value:
\label{lem:hklm} \verb+KkLM\+ system \land current control set \verb+ services \land dns cache \land parameters [register reverse lookup] \\
  Queries value:
Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[registerwanadapters]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [registration ttl]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
  Queries value:
Queries 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]
  Queries value:
```

HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] HKLM\svstem\currentcontrolset\services\dnscache\parameters[maxcachesize] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [maxnegative cachettl]$ Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[queryadaptername] Queries value: c7d49d7cecdc}[disableadapterdomainname] Oueries value: c7d49d7cecdc}[registrationenabled] Queries value: c7d49d7cecdc}[registeradaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[registrationmaxaddresscount] Queries value: c7d49d7cecdc}[maxnumberofaddressestoregister] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[domain] Queries value: c7d49d7cecdc}[dhcpdomain] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[ipautoconfigurationenabled] Oueries value: $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4300-abe3-4300-a$ c7d49d7cecdc}[addresstype] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[nameserver] Oueries value: $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4300-abe3-4300-a$ c7d49d7cecdc}[dhcpnameserver] HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist] Queries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder] HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong Oueries value: cryptographic provider[type] HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong Oueries value: cryptographic provider[image path] ${\tt HKLM \ } system \verb| current control set \verb| control \ \\ session$ Queries value: manager[safeprocesssearchmode] HKLM\software\microsoft\cryptography[machineguid] Oueries value: Queries value: HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45ab78-1084642581fb]

HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-Oueries value:

0000-00000000000000

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

Oueries value: HKCR\clsid\{00021401-0000-0000-c000-

00000000046}\inprocserver32[inprocserver32]

HKCR\clsid\{00021401-0000-0000-c000-00000000046}\inprocserver32[] Queries value:

HKCR\clsid\{00021401-0000-0000-c000-00000000046}[appid] Oueries value:

Oueries value: HKCR\clsid\{00021401-0000-0000-c000-

00000000046}\inprocserver32[threadingmodel]

Oueries value:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [compare junctionness]$

Queries value: HKCR\network\sharinghandler[]
Queries value: HKLM\software\microsoft\windows

nt\currentversion\winlogon[userenvdebuglevel]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\winlogon[chkaccdebuglevel]

Queries value: HKLM\system\currentcontrol\set\control\productoptions[producttype]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[local settings]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\winlogon[rsopdebuglevel]

Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]

Queries value:

HKLM\system\currentcontrolset\services\lanmanserver\defaultsecurity[srvsvcdefaultshareinfo]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[start menu]

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

folders[common start menu]

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

folders[common appdata]

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

folders[appdata]

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

folders[my pictures]

Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir (x86)]
Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell

folders[commonpictures]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\profilelist[profilesdirectory]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\profilelist[allusersprofile]

Queries value: HKCR\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\inprocserver32[]

Queries value:

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

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

folders[commonmusic]

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

folders[commonvideo]

Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
Queries value: HKCU\software\microsoft\ctf[disable thread input manager]

Queries value: HKCR\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\inprocserver32[inprocserver32]

 $\label{lem:queries value: HKCR\clsid {8856f961-340a-11d0-a96b-00c04fd705a2} \\ \noalign{\color=0.9\textwidth} \noalign{\color=0.9\textwi$

 $Queries\ value: \qquad \qquad \text{HKCR} \\ \text{Clsid} \\ \text{\{8856f961-340a-11d0-a96b-00c04fd705a2\}[appid]}$

Queries value: HKCR\clsid\{8856f961-340a-11d0-a96b-

 ${\tt 00c04fd705a2} \verb|\inprocserver32[threading model]$

Queries value: HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe[] Queries value: HKLM\software\microsoft\internet explorer\setup[iexplorelastmodifiedlow]

Queries value: HKLM\software\microsoft\internet

explorer\setup[iexplorelastmodifiedhigh]

Queries value: HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib[]
Queries value: HKLM\software\microsoft\internet explorer\setup[installstarted]

Queries value: HKCR\clsid\{9ba05972-f6a8-11cf-a442-

00a0c90a8f39}\inprocserver32[inprocserver32]

 $Queries\ value: \\ HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\ \ linprocserver32[]$

Queries value: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}[appid]

Queries value: HKCR\clsid\{9ba05972-f6a8-11cf-a442-

00a0c90a8f39}\inprocserver32[threadingmodel]

Queries value: HKLM\software\microsoft\ole[maximumallowedallocationsize]
Queries value: HKLM\software\microsoft\ole[defaultaccesspermission]

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

Queries value: HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32[]

Queries value: HKCR\clsid\{00020424-0000-0000-c000-

00000000046}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprocserver32[]

Queries value: HKCR\clsid\{00020424-0000-0000-c000-00000000046}[appid]

Queries value: HKCR\clsid\{00020424-0000-0000-c000-

00000000046}\inprocserver32[threadingmodel]

Queries value: HKLM\software\microsoft\rpc[udtalignmentpolicy]

Queries value: HKCR\interface\{00020400-0000-0000-000000000046}\proxystubclsid32[]

Queries value: HKCR\clsid\{00020420-0000-0000-c000-

00000000046}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{00020420-0000-0000-00000000046}\inprocserver32[]

Queries value: HKCR\clsid\{00020420-0000-0000-000000000046}[appid]

Queries value: HKCR\clsid\{00020420-0000-0000-

```
00000000046}\inprocserver32[threadingmodel]
                         HKCU\software\microsoft\internet explorer\main[frametabwindow]
 Oueries value:
 Oueries value:
                          HKLM\software\microsoft\internet explorer\main[frametabwindow]
                          HKCU\software\microsoft\internet explorer\main[framemerging]
 Queries value:
                          HKLM\software\microsoft\internet explorer\main[framemerging]
 Oueries value:
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[sessionmerging]
 Oueries 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]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
 Queries value:
                          HKLM\software\microsoft\internet explorer\main[tabprocgrowth]
 Queries value:
                          HKLM\software\microsoft\internet explorer\main[navigationdelay]
                          HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[]
 Oueries value:
 Queries value:
                          HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[loadwithoutcom]
                         HKLM\software\microsoft\windows\currentversion\shell
 Oueries value:
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
 Oueries value:
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}
0x401]
                         HKCU\software\microsoft\windows\currentversion\shell
 Queries value:
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}
                         HKCR\clsid\{871c5380-42a0-1069-a2ea-
 Oueries value:
08002b30309d}\inprocserver32[inprocserver32]
                         HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[appid]
 Oueries value:
                         HKCR\clsid\{871c5380-42a0-1069-a2ea-
 Queries value:
08002b30309d}\inprocserver32[threadingmodel]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[secureprotocols]
                         HKLM\software\policies\microsoft\internet
 Queries value:
explorer\main[security_hklm_only]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[idnenabled]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
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]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[disablebasicoverclearchannel]
                         HKCU\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol[feature clientauthcertfilter]
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[syncmode5]
                          HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
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]
                         \label{lem:hklm} \verb+ HKLM \+ software \+ microsoft \+ windows \+ current version \+ internet
 Oueries value:
settings\5.0\cache\content[peruseritem]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cacheprefix]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\content[cachelimit]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\cookies[cacheprefix]
```

```
Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cachelimit]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\history[peruseritem]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\history[cachelimit]
                            \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ 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
 Oueries 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]
                            \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Oueries 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]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
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]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachelimit]
 Queries value:
                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\ietld[cacherepair]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings\5.0\cache\extensible cache\ietld[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\ietld[cachelimit]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[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\extensible cache\mshist012014041220140413[cachelimit]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\privacie:[cacherepair]
 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\extensible cache\privacie:[cachepath]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\privacie:[cachelimit]
 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\extensible cache\privacie:[cacheoptions]
```

 $\label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\$

Queries value:

```
settings[disableworkerthreadhibernation]
                              HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[disableworkerthreadhibernation]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
  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[socketsendbufferlength]
                              \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}.
  Oueries value:
settings[socketreceivebufferlength]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[keepalivetimeout]
  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[maxhttpredirects]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
                              HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[maxconnectionsperserver]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Queries value:
                              HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[maxconnectionsperproxy]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[serverinfotimeout]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[connecttimeout]
                              HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[connecttimeout]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[connectretries]
                              HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[connectretries]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[sendtimeout]
                              HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[sendtimeout]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
                              HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[receivetimeout]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablentlmpreauth]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[certcachenovalidate]
  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[scavengecachefilelifetime]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                              \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
  Oueries value:
settings\5.0\cache[scavengecachefilelimit]
  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[httpdefaultexpirytimesecs]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
                              HKLM\software\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[downloadmanager.exe]
                              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature disable unicode handle closing callback[*]
  Oueries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
                              HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[perusercookies]
                              HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[leashlegacycookies]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[disablent4rascheck]
                              HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[dialupuselansettings]
                              HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[dialupuselansettings]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
                              HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[bypassftptimecheck]
  Oueries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduringauth]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
                              HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[releasesocketduring401auth]
```

```
Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
                          HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablelegacypreauthasserver]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasshttpnocachecheck]
                          HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasshttpnocachecheck]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
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
 Oueries value:
settings[nocheckautodialoverride]
                          HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[nocheckautodialoverride]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dontusednsloadbalancing]
 Oueries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
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
 Oueries value:
settings[dnscacheentries]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dnscachetimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonpost]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnalwaysonpost]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonzonecrossing]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertsending]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonbadcertrecving]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonhttpstohttpredirect]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
                          HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[urlencoding]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[truncatefilename]
                          \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[badproxyexpirestime]
 Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nofilemenu]
                          HKLM\software\microsoft\windows\currentversion\policies\ratings[key]
 Queries value:
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[urlencoding]
                          HKCU\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[downloadmanager.exe]
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[downloadmanager.exe]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
 Oueries value:
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave31
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave91
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
 Oueries 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[midi5]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
 Oueries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
 Oueries value:
 Queries 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]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
 Queries value:
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
 Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ telephony \ [tapi32 max numrequest retries]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32requestretrytimeout]
                           HKLM\software\microsoft\tracing[enableconsoletracing]
 Queries value:
 Queries value:
                           HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
 Oueries value:
                           HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
                           HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
 Queries value:
                           HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
 Oueries value:
 Oueries value:
                           HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
                           HKLM\software\microsoft\tracing\rasapi32[filedirectory]
 Queries value:
 Queries value:
                           HKLM\software\microsoft\windows
nt\currentversion\profilelist[defaultuserprofile]
                           HKLM\software\microsoft\windows\currentversion[commonfilesdir]
 Queries value:
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[profileimagepath]
 Oueries value:
                           HKCU\software\microsoft\windows
nt\currentversion\winlogon[parseautoexec]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[proxyenable]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[autoconfigurl]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacvsettings]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zonemap[autodetect]
                           HKCU\software\microsoft\internet explorer[no3dborder]
 Queries value:
 Oueries value:
                           HKLM\software\microsoft\internet explorer[no3dborder]
 Queries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[downloadmanager.exe]
                          HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_mime_handling[*]
 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\user agent[]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\user agent[compatible]
 Queries value:
                           \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
settings\5.0\user agent[compatible]
 Queries value:
                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings\5.0\user agent[version]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
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
```

HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]

Oueries value:

```
settings\5.0\user agent[platform]
                         HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\user agent[platform]
 Queries value:
                         HKLM\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature_max connections perserver [download manager.exe]| \\
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[*]
                        HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[downloadmanager.exe]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[*]
```

Queries value: HKCU\software\microsoft\internet explorer\international[acceptlanguage]

Oueries value: HKCR\clsid\{d3388703-5092-487c-8217-

11ada1ca68b5}\localserver32[localserver32]

Queries value: HKCR\clsid\{d3388703-5092-487c-8217-11ada1ca68b5}\localserver32[]

Oueries value: HKLM\software\microsoft\rpc\securityservice[10] Oueries value:

HKLM\system\currentcontrolset\control\securityproviders[securityproviders]

Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]

Oueries value:

HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]

Queries value:

HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]

Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]

Queries value:

HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[version]

Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]

Queries value:

HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]

Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]

Queries value:

Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid] HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version] Oueries value: Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]

Queries value:

HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize]

HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment] Queries value:

Oueries value:

HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities]

Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid] HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version] Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type] Oueries value:

Queries value:

 $HKLM \setminus system \setminus current control \\ lsa \setminus sspicache \setminus msnsspc. \\ dll[tokensize]$ Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\zones\3[1a10]

Queries value: HKCR\mime\database\content type\text/html[extension]

HKLM\software\microsoft\internet Oueries value:

explorer\main\featurecontrol\feature_mime_sniffing[downloadmanager.exe]

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

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

settings[istextplainhonored]

HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_feeds[downloadmanager.exe] HKLM\software\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_feeds[*]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_safe_bindtoobject[downloadmanager.exe]

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

00aa00686f13}\inprocserver32[inprocserver32]

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

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

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

00aa00686f13}\inprocserver32[threadingmodel]

HKLM\software\microsoft\internet Queries value:

explorer\main\featurecontrol\feature_legacy_dispparams[downloadmanager.exe]

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

explorer\main\featurecontrol\feature_object_caching[downloadmanager.exe]

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

HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay] Oueries value:

Oueries value: HKLM\software\microsoft\internet explorer\application

compatibility[downloadmanager.exe]

Oueries value: HKCU\software\microsoft\internet explorer\domstorage[totallimit] Queries value: HKCU\software\microsoft\internet explorer\domstorage[domainlimit] Queries value: HKCU\software\microsoft\windows

nt\currentversion\windows[dragscrollinset]

Queries value: HKCU\software\microsoft\windows

nt\currentversion\windows[dragscrolldelay]

Queries value: HKCU\software\microsoft\windows

nt\currentversion\windows[dragscrollinterval]

Queries value: HKLM\software\microsoft\internet

 $\verb|explorer| \verb|main| featurecontrol| feature_restrict_filedownload[| download|| manager.exe]| \\$

Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_filedownload[*]
Queries value: HKCR\protocols\handler\about[clsid]
Queries value: HKCR\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]

Queries value: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}[appid]

Queries value: HKCR\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\inprocserver32[threadingmodel]

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

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[]

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

history[daystokeep]

Queries value: HKLM\software\policies\microsoft\internet explorer[smartdithering]

Queries value: HKCU\software\microsoft\internet explorer[smartdithering]

Queries value: HKCU\software\microsoft\internet explorer[rtfconverterflags]

Queries value: HKLM\software\policies\microsoft\internet explorer\main[usecleartype]

Queries value: HKCU\software\microsoft\internet explorer\main[usecleartype]

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

explorer\main[page_transitions]

Queries value: HKCU\software\microsoft\internet explorer\main[page_transitions]

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

explorer\main[use_dlgbox_colors]

Queries value: HKCU\software\microsoft\internet explorer\main[use_dlgbox_colors] Queries value: HKLM\software\policies\microsoft\internet explorer\main[anchor

underline]

Queries value: HKCU\software\microsoft\internet explorer\main[anchor underline]
Queries value: HKCU\software\microsoft\internet explorer\main[css_compat]
Queries value: HKCU\software\microsoft\internet explorer\main[expand alt text]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[display inline

images]

Queries value: HKCU\software\microsoft\internet explorer\main[display inline images]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[display inline

videos]

Queries value: HKCU\software\microsoft\internet explorer\main[display inline videos]

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

explorer\main[play_background_sounds]

Queries value: HKCU\software\microsoft\internet explorer\main[play_background_sounds]
Queries value: HKLM\software\policies\microsoft\internet explorer\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]

Queries value: HKLM\software\policies\microsoft\internet explorer\main[smoothscroll]

Queries value: HKCU\software\microsoft\internet explorer\main[smoothscroll]

Queries 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

placeholders]

Queries value: HKCU\software\microsoft\internet explorer\main[show image placeholders]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[disable script]

debugger]

Queries value: HKCU\software\microsoft\internet explorer\main[disable script debugger]
Queries value: HKCU\software\microsoft\internet explorer\main[disablescriptdebuggerie]
Queries value: HKCU\software\microsoft\internet explorer\main[move system caret]
Queries value: HKCU\software\microsoft\internet explorer\main[force offscreen

composition]

Queries value: HKLM\software\policies\microsoft\internet explorer\main[enable

autoimageresize]

Queries value: HKCU\software\microsoft\internet explorer\main[enable autoimageresize]

Queries value: HKCU\software\microsoft\internet explorer\main[usethemes]
Queries value: HKCU\software\microsoft\internet explorer\main[useth]
Queries value: HKCU\software\microsoft\internet explorer\main[q300829]
Queries value: HKCU\software\microsoft\internet explorer\main[cleanup htcs]

Queries value: HKLM\software\policies\microsoft\internet explorer\main[xdomainrequest]

 Queries value: HKCU\software\microsoft\internet

explorer\international[default_codepage]

Queries value: HKCU\software\microsoft\internet explorer\international[autodetect]

Queries value: HKCU\software\microsoft\internet
explorer\international\scripts[default_iefontsizeprivate]

Queries value: HKCU\software\microsoft\internet explorer\settings[anchor color]

Queries value: HKCU\software\microsoft\internet explorer\settings[anchor color visited]
Queries value: HKCU\software\microsoft\internet explorer\settings[anchor color hover]
Queries value: HKCU\software\microsoft\internet explorer\settings[always use my colors]
Queries value: HKCU\software\microsoft\internet explorer\settings[always use my font

size]

Queries value: HKCU\software\microsoft\internet explorer\settings[always use my font

face]

Queries value: HKCU\software\microsoft\internet explorer\settings[disable visited

hyperlinks]

Queries value: HKCU\software\microsoft\internet explorer\settings[use anchor hover

color]
Queries value: HKCU\software\microsoft\internet explorer\settings[miscflags]
Queries value: HKCU\software\microsoft\windows\currentversion\policies[allow]

programmatic cut_copy_paste]

Queries value: HKLM\system\currentcontrolset\control\nls\codepage[950]

Queries value: HKCU\software\microsoft\internet

explorer\international\scripts\3[iefontsize]

Queries value: HKCU\software\microsoft\internet
explorer\international\scripts\3[iefontsizeprivate]
 Queries value: HKCU\software\microsoft\internet
explorer\international\scripts\3[iepropfontname]

Queries value: HKCU\software\microsoft\internet

explorer\international\scripts\3[iefixedfontname]

Queries value: HKLM\software\microsoft\internet explorer\version vector[vml]
Queries value: HKLM\software\microsoft\internet explorer\version vector[ie]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_zone_elevation[downloadmanager.exe]

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

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

settings\zones\3[2700]

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

settings\zones\3[2700]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_xssfilter[downloadmanager.exe]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_xssfilter[*]

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

settings\zones[securitysafe]

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

settings\zones\3[1400]

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

settings[warnonintranet]

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

settings[warnonintranet]

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

f4ceaaf59cfc}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32[]

Queries value: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[appid]

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

f4ceaaf59cfc}\inprocserver32[threadingmodel]

 $\label{lem:queries value: HKLM\software\microsoft\tf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}\ensuremath{[enable]}$

Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-

431b3828ba53}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32[]

Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}[appid]

Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-

431b3828ba53}\inprocserver32[threadingmodel]

Queries value: HKCR\clsid\{a4b544a1-438d-4b41-9325-

869523e2d6c7}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserver32[]

Queries value: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}[appid]

Queries value: HKCR\clsid\{a4b544a1-438d-4b41-9325-

869523e2d6c7}\inprocserver32[threadingmodel]

Queries value: $\label{lem:hatcosoft} $$\operatorname{Arcosoft}\left(\frac{1}{78cb500e-26ed-4fcc-854c-77e8f3d1aa80}\cdot \frac{5130a009-5540-4fcf-97eb-aad33fc0ee09}[description] $$ Queries value: <math display="block"> \label{lem:hatcosoft} \left(\frac{1}{78cb500e-26ed-4fcc-854c-77e8f3d1aa80}\cdot \frac{7ae86bb7-262c-431e-9111-c974b6b7cac3}[description] $$ Queries value: <math display="block"> \label{lem:hatcosoft} \left(\frac{1}{78cb500e-26ed-4fcc-854c-77e8f3d1aa80}\cdot \frac{1}{6c6ebc0a-f2b2-4f17-930e-ca9faff4cd04}[description] $$ \label{lem:hatcosoft} \left(\frac{1}{78cb500e-26ed-4fcc-854c-77e8f3d1aa80}\cdot \frac{1}{6c6ebc0a-f2b2-4f17-930e-ca9faff4cd04}[description] $$ \label{lem:hatcosoft} \left(\frac{1}{78cb500e-26ed-4fcc-854c-77e8f3d1aa80}\cdot \frac{1}{6c6ebc0a-f2b2-4f17-930e-ca9faff4cd04}[description] $$ \label{lem:hatcosoft} \right) $$ \label{lem:hatcosoft} $$ \label{lem:hatcosoft} \left(\frac{1}{78cb500e-26ed-4fcc-854c-77e8f3d1aa80}\cdot \frac{1}{6c6ebc0a-f2b2-4f17-930e-ca9faff4cd04}[description] $$ \label{lem:hatcosoft} \right) $$ \label{lem:hatcosoft} $$ \label{lem:hatcosoft} $$ \label{lem:hatcosoft} $$ \label{lem:hatcosoft} \left(\frac{1}{78cb500e-26ed-4fcc-854c-77e8f3d1aa80}\cdot \frac{1}{6c6ebc0a-f2b2-4f17-930e-ca9faff4cd04}[description] $$ \label{lem:hatcosoft} $$ \label{lem:hatcos$

Queries value: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-

00aa00bbbb58}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32[]

Queries value: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}[appid]

Queries value: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-

00aa00bbbb58}\inprocserver32[threadingmodel]

```
Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1201]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\language groups[1]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
  Oueries value:
                                     HKLM\software\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
  Queries value:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown[downloadmanager.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\zones\3[2000]
  Queries value:
                                     HKLM\software\microsoft\internet explorer\feed discovery[sound]
                                     HKCU\software\microsoft\ftp[use web based ftp]
  Oueries value:
  Queries value:
                                     HKLM\software\microsoft\internet explorer\main[maxrenderline]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
                                     HKCU\control panel\desktop[lamebuttontext]
  Oueries value:
  Queries value:
                                     HKCR\mime\database\content type\image/png[extension]
  Queries value:
                                     HKCR\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[inprocserver32]
  Queries value:
                                     HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[]
  Queries value:
                                     HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}[appid]
  Oueries value:
                                     HKCR\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[threadingmodel]
  Queries value:
                                     HKCR\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32[inprocserver32]
                                     HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32[]
  Queries value:
  Queries value:
                                     HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}[appid]
                                     HKCR\clsid\{6a01fda0-30df-11d0-b724-
  Oueries value:
00aa006c1a01}\inprocserver32[threadingmodel]
                                     HKCR\mime\database\content type\image/bmp\bits[0]
  Oueries value:
                                     HKCR\mime\database\content type\image/gif\bits[0]
  Oueries value:
  Queries value:
                                     HKCR\mime\database\content type\image/jpeg\bits[0]
  Queries value:
                                     HKCR\mime\database\content type\image/pjpeg\bits[0]
                                     HKCR\mime\database\content type\image/png\bits[0]
  Oueries value:
                                     HKCR\mime\database\content type\image/x-png\bits[0]
  Queries value:
                                     HKCR\mime\database\content type\image/x-wmf\bits[0]
  Oueries value:
                                     HKCR\mime\database\content type\image/x-png[image filter clsid]
  Oueries value:
                                     HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
  Oueries value:
00a0c913f750}\inprocserver32[inprocserver32]
                                     HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[]
  Queries value:
  Queries value:
                                     HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}[appid]
                                     HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
  Oueries value:
00a0c913f750}\inprocserver32[threadingmodel]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\zones\3[1c00]
                                     HKCU\software\microsoft\internet
  Queries value:
explorer\ietld\lowmic[ietlddllversionlow]
                                     HKCU\software\microsoft\internet
  Oueries value:
explorer\ietld\lowmic[ietlddllversionhigh]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[{aeba21fa-782a-4a90-978d-b72164c80120}]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[privacyadvanced]
  Queries value:
                                     HKCU\software\microsoft\internet
explorer\services[selectionactivitybuttondisable]
                                     HKCU\software\microsoft\internet explorer\suggested sites[enabled]
  Queries value:
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[allowclsidprogidmapping]
                                     HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[docobject]
  Oueries value:
  Queries value:
                                     HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[browseinplace]
                                     HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[isshortcut]
  Oueries value:
  Queries value:
                                     \label{local-equation} $HKCR\clsid{ff393560-c2a7-11cf-bff4-444553540000}[always showext]$
                                     HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[nevershowext]
  Oueries value:
                                     Queries value:
                                     HKCR \ clsid \ \{ff393560-c2a7-11cf-bff4-
  Oueries value:
444553540000}\inprocserver32[loadwithoutcom1
  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}
0x4011
                                     HKCU\software\microsoft\windows\currentversion\shell
extensions \\ \\ cached [\{ff393560-c2a7-11cf-bff4-444553540000\} \\ \\ \{e022b1e2-a19e-4b43-8160-7bcecacb3d6e\} \\ \\ \\ extensions \\ \\ \\ extensions 
0x4011
```

```
HKCR\clsid\{ff393560-c2a7-11cf-bff4-
  Oueries value:
444553540000}\inprocserver32[inprocserver32]
                                   HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[appid]
  Oueries value:
                                   HKCR\clsid\{ff393560-c2a7-11cf-bff4-
  Queries value:
444553540000}\inprocserver32[threadingmodel]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042820160429[cacherepair]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\mshist012016042820160429[cachepath]
  Oueries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042820160429[cacheprefix]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042820160429[cachelimit]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\mshist012016042820160429[cacheoptions]
  Queries value:
                                   HKCU\software\microsoft\internet
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-
  Oueries value:
08002b30309d}\shellfolder[callforattributes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}]
  Queries value:
                                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hidefolderverbs]
                                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[localizedstring]
  Queries value:
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[flags]
                                   HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
  Queries value:
1757981266-507921405-1957994488-1003[state]
                                   HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
  Oueries value:
1757981266-507921405-1957994488-1003[userpreference]
                                   HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
  Queries value:
1757981266-507921405-1957994488-1003[centralprofile]
                                   \label{lem:hklm} \mbox{ HKLM} \mbox{ hicrosoft} \mbox{ windows nt} \mbox{ currentversion} \mbox{ profilelist} \mbox{ s-1-5-21-1} \mbox{ of tware} \mbox{ windows nt} \mbox{ of tware} \mbox{ of
  Queries value:
1757981266-507921405-1957994488-1003[profileloadtimelow]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[profileloadtimehigh]
  Queries value:
HKCU \ software \ microsoft \ windows \ shell no roam \ muicache [@c:\ windows \ system 32 \ shell 32.dll, -9216]
                                   HKCR\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32[inprocserver32]
                                   HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32[]
  Queries value:
  Queries value:
                                   HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}[appid]
                                   HKCR\clsid\{275c23e2-3747-11d0-9fea-
  Oueries value:
00aa003f8646}\inprocserver32[threadingmodel]
                                   HKLM\system\currentcontrolset\control\nls\codepage[1250]
  Queries value:
  Oueries value:
                                   HKLM\svstem\currentcontrolset\control\nls\codepage[1251]
  Queries value:
                                   HKLM\system\currentcontrolset\control\nls\codepage[1253]
                                   HKLM\system\currentcontrolset\control\nls\codepage[1254]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\nls\codepage[1255]
  Oueries value:
  Oueries value:
                                   HKLM\system\currentcontrolset\control\nls\codepage[1256]
                                   HKLM\system\currentcontrolset\control\nls\codepage[1257]
  Queries value:
  Queries value:
                                   HKLM\system\currentcontrolset\control\nls\codepage[1258]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\nls\codepage[874]
                                   HKLM\system\currentcontrolset\control\nls\codepage[932]
  Queries value:
  Queries value:
                                   HKLM\system\currentcontrolset\control\nls\codepage[936]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\nls\codepage[949]
                                   HKLM\system\currentcontrolset\control\nls\codepage[1361]
  Oueries value:
  Sets/Creates value:
HKCU \ software \ microsoft \ windows \ shell no roam \ muicache \ [c:\docume-1\admin\locals-1\temp\download manager.exe]
  Sets/Creates value:
                                   HKCR\clsid\{d3388703-5092-487c-8217-11ada1ca68b5}[]
  Sets/Creates value:
                                   HKCR\clsid\{d3388703-5092-487c-8217-11ada1ca68b5}\localserver32[]
                                   HKCR\clsid\{d3388703-5092-487c-8217-
  Sets/Creates value:
11ada1ca68b5}\localserver32[serverexecutable]
  Sets/Creates value:
                                   HKCR\clsid\{d3388703-5092-487c-8217-11ada1ca68b5}\typelib[]
  Sets/Creates value:
                                   HKCR\clsid\{d3388703-5092-487c-8217-11ada1ca68b5}\version[]
  Sets/Creates value:
                                   HKCR\typelib\{dcabb943-792e-44c4-9029-ecbee6265af9}\1.0[]
  Sets/Creates value:
                                   HKCR\typelib\{dcabb943-792e-44c4-9029-ecbee6265af9}\1.0\flags[]
  Sets/Creates value:
                                   HKCR\typelib\{dcabb943-792e-44c4-9029-ecbee6265af9}\1.0\0\win32[]
                                   HKCR\typelib\{dcabb943-792e-44c4-9029-ecbee6265af9}\1.0\helpdir[]
  Sets/Creates value:
  Sets/Creates value:
                                   HKCR\interface\{3408ac0d-510e-4808-8f7b-6b70b1f88534}[]
  Sets/Creates value:
                                   HKCR\interface\{3408ac0d-510e-4808-8f7b-6b70b1f88534}\proxystubclsid[]
  Sets/Creates value:
                                   HKCR \verb|\interface| \{3408ac0d-510e-4808-8f7b-6b70b1f88534\} \verb|\proxystubclsid32[]| \\
                                   HKCR\interface\{3408ac0d-510e-4808-8f7b-6b70b1f88534}\typelib[]
  Sets/Creates value:
  Sets/Creates value:
                                   HKCR \ interface \ \{3408ac0d-510e-4808-8f7b-6b70b1f88534\} \ typelib[version]
```

Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016042820160429[cachepath] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016042820160429[cacheprefix] HKCU\software\microsoft\windows\currentversion\internet Sets/Creates value: settings\5.0\cache\extensible cache\mshist012016042820160429[cachelimit] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016042820160429[cacheoptions] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016042820160429[cacherepair] HKLM\software\microsoft\cryptography\rng[seed] Value changes: Value changes: $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mountpoints \\ 2 \setminus \{f90255c2-6bc4-11e3-9fc7-12e3-12e4\} \setminus \{f90255c2-6bc4-11e3-9fc7-12e4\} \setminus \{f90255c2-6bc4-12e4\} \setminus \{f9025c2-6bc4-12e4\} \setminus \{f9025c2-6bc4-12e4\} \setminus \{f9025c2-6bc4-12e4\} \setminus \{f9025c2-6bc4-12e4\} \setminus \{f9025c2-6bc4-1$ 806d6172696f}[baseclass] $\label{lem:hkcu} \verb+KKCU\+software\+microsoft\+windows\+currentversion\+explorer\+shell$ Value changes: folders[personal] Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell folders[common documents] Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[desktop] Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell folders[common desktop] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\zonemap[proxybypass] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[intranetname] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\zonemap[uncasintranet] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\zonemap[autodetect] HKCU\software\microsoft\windows\currentversion\explorer\shell Value changes: folders[cache] Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cookies] $\label{local-constraint} \mbox{HKCU\software\mbox{\sc urrentversion\explorer\shell}} \mbox{}$ Value changes: folders[start menu] HKLM\software\microsoft\windows\currentversion\explorer\shell Value changes: folders[common start menu] HKLM\software\microsoft\windows\currentversion\explorer\shell Value changes: folders[common appdata] Value changes: $\label{local-constraint} \mbox{HKCU\software\mbox{\sc urrentversion\explorer\shell}} \mbox{}$ folders[appdata] HKCU\software\microsoft\windows\currentversion\explorer\shell folders[mv Value changes: pictures] HKLM\software\microsoft\windows\currentversion\explorer\shell Value changes: folders[commonpictures] Value changes: $\label{lem:hklm} \verb+Kklm\+ software\+ icrosoft\+ windows\+ current version\+ explorer\+ shell$ folders[commonmusic] Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell folders[commonvideo] HKCU\software\microsoft\windows\currentversion\explorer\shell Value changes: folders[history]

Value changes:

HKCU\software\microsoft\windows\currentversion\internet settings[proxyenable]

Value changes:

settings\connections[savedlegacysettings]

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\extensible cache\mshist012016042820160429[cachepath]

Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[favorites]

Value changes: HKCU\software\microsoft\internet explorer\main\windowssearch[version]

HKCU\software\microsoft\windows\currentversion\internet