Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 5, Task ID: 18

Task ID: 18 Risk Level: 5

Date Processed: 2016-04-28 12:46:41 (UTC)

Processing Time: 62.28 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\700aa61e9dbd14abfcc633546a5be910.exe"

Sample ID: 5
Type: basic
Owner: admin

Label: 700aa61e9dbd14abfcc633546a5be910

Date Added: 2016-04-28 12:44:50 (UTC)
File Type: PE32:win32:gui

File Type: PE32:win32:gui File Size: 673560 bytes

MD5: 700aa61e9dbd14abfcc633546a5be910

SHA256: 129286051a8bdcd2a27601d98ae44002bfc430fe0d98f3307de97b15ec75bc65

Description: None

Pattern Matching Results

5 Creates shortcut on desktop

3 Long sleep detected

3 Creates a file extension shortcut

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

Writes to a log file [Info]

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

Creates process: C:\WINDOWS\Temp\700aa61e9dbd14abfcc633546a5be910.exe

["c:\windows\temp\700aa61e9dbd14abfcc633546a5be910.exe"]

Creates process: C:\WINDOWS\Temp\700aa61e9dbd14abfcc633546a5be910.exe
["c:\windows\temp\700aa61e9dbd14abfcc633546a5be910.exe" /_ShowProgress]
Loads service: RASMAN [C:\WINDOWS\system32\svchost.exe -k netsvcs]
Terminates process: C:\WINDOWS\Temp\700aa61e9dbd14abfcc633546a5be910.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: \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\ZonesCacheCounterMutex
Creates mutex: \BaseNamedObjects\!PrivacIE!SharedMemory!Mutex

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\MSIMGSIZECacheMutex
Creates mutex: \BaseNamedObjects\WininetConnectionMutex
Creates mutex: \BaseNamedObjects\MSCTF.Shared.MUTEX.MN

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

Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

Creates semaphore: \BaseNamedObjects\1VtP0S1F102ZtG0W1T1C1PtP1V

 $\label{local-control} $$\operatorname{Semaphore:}$ $$\operatorname{Semaphore:}$$

File System Events

Creates: C:\Documents and Settings\Admin\Local Settings\Temp\00A5A36F.log
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css

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

 $Settings \verb|\Temp\ish10855279\css\ie6_main.css|$

```
Creates:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\css\main.css
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
 Creates:
ui
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\browse.css
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\button.css
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\checkbox.css
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
 Creates:
ui\images
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\images\button-bg.png
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
 Creates:
ui\images\progress-bg-corner.png
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
 Creates:
ui\images\progress-bg.png
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\images\progress-bg2.png
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
 Creates:
ui\progress-bar.css
                         C:\Documents and Settings\Admin\Local
 Creates:
Settings\Temp\ish10855279\csshover3.htc
                         C:\Documents and Settings\Admin\Local
 Creates:
Settings\Temp\ish10855279\form.bmp.Mask
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\images
 Creates:
                         C:\Documents and Settings\Admin\Local
 Creates
Settings\Temp\ish10855279\images\BG.png
                         C:\Documents and Settings\Admin\Local
 Creates:
Settings\Temp\ish10855279\images\Close.png
                         C:\Documents and Settings\Admin\Local
 Creates:
Settings\Temp\ish10855279\images\Close_Hover.png
 Creates:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Color_Button.png
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Color_Button_Hover.png
                         C:\Documents and Settings\Admin\Local
 Creates:
Settings\Temp\ish10855279\images\Grey_Button.png
                         C:\Documents and Settings\Admin\Local
 Creates:
Settings\Temp\ish10855279\images\Grey_Button_Hover.png
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Icon_Generic.png
 Creates:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Loader.gif
                         C:\Documents and Settings\Admin\Local
 Creates:
Settings\Temp\ish10855279\images\Pause_Button.png
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Progress.png
                         C:\Documents and Settings\Admin\Local
 Creates:
Settings\Temp\ish10855279\images\ProgressBar.png
                         C:\Documents and Settings\Admin\Local
 Creates:
Settings\Temp\ish10855279\images\Quick_Specs.png
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Resume_Button.png
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\locale
                         C:\Documents and Settings\Admin\Local
 Creates
Settings\Temp\ish10855279\locale\DE.locale
                         C:\Documents and Settings\Admin\Local
 Creates:
Settings\Temp\ish10855279\locale\EN.locale
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\sdk
 Creates:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\sdk\exceptlist.txt
                         C:\Documents and Settings\Admin\Local
 Creates:
Settings \verb|\Temp\ish10855279\bootstrap_3733.html| \\
                         C:\Documents and Settings\Admin\Local Settings\Temp\00A69D39.log
 Creates:
                         C:\Documents and Settings\Admin\Local
Settings \verb|\Temp\ICReinstall_700| aa 61e 9dbd 14abfcc 633546a 5be 910.exe
 Creates:
                         C:\Documents and Settings\Admin\Desktop\Continue CCleaner
Installation.lnk
 Creates:
                         C:\Documents and Settings\Admin\Local Settings\Temp\00A6A078.log
                         C:\Documents and Settings\Admin\Local Settings\Temp\is956058749
 Creates:
                         C:\Documents and Settings\Admin\Local
 Creates:
{\tt Settings\Temp\is956058749\10920075\_Setup.EXE}
 Opens:
                         C:\WINDOWS\Prefetch\700AA61E9DBD14ABFCC633546A5BE-0CD25A82.pf
 Opens:
                         C:\Documents and Settings\Admin
 Opens:
                         C:\WINDOWS\system32\imm32.dl1
 Opens:
                         C:\WINDOWS\system32\comctl32.dll
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Config
 Opens:
                         C:\WINDOWS\Temp\700aa61e9dbd14abfcc633546a5be910.exe
                         C:\WINDOWS\svstem32\shell32.dll
 Opens:
```

C:\WINDOWS\system32\SHELL32.dll.124.Manifest

Opens:

```
C:\WINDOWS\system32\SHELL32.dll.124.Config
  Opens:
                                      C:\WINDOWS\WinSxS\x86 Microsoft.Windows.Common-
  Opens:
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
  Opens:
                                      C:\WINDOWS\WindowsShell.Config
                                      C:\WINDOWS\system32\URLMON.DLL.123.Manifest
  Opens:
  Opens:
                                      C:\WINDOWS\system32\URLMON.DLL.123.Config
  Opens:
                                      C:\WINDOWS\system32\wininet.dll.123.Manifest
  Opens:
                                      C:\WINDOWS\system32\wininet.dll.123.Config
  Opens:
                                      C:\WINDOWS\system32\olepro32.dll
  Opens:
                                      C:\WINDOWS\system32\rpcss.dll
                                      C:\WINDOWS\system32\MSCTF.dll
  Opens:
  Opens:
                                      C:\WINDOWS\system32\MSCTFIME.IME
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Temp
                                      C:\Documents and Settings\Admin\Local Settings\Temp\00A5A36F.log
  Opens:
  Opens:
                                      C:\WINDOWS\Temp\2b018457-30d9-4422-b29c-98224f056ad2
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css
                                      C:\Documents and Settings\Admin\Local
  Opens:
Settings\Temp\ish10855279\css\ie6_main.css
                                      C:\Documents and Settings\Admin\Local
  Opens:
Settings\Temp\ish10855279\css\main.css
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui
  Opens:
                                      \label{lem:local_Settings} C: \Documents \ and \ Settings \Admin\Local \ Settings \Temp\ \S55279\ \Css\ \Sdk-resp. \ \Colored \Local \ \Settings \ \Css\ \Sdk-resp. \ \Css\ \Sdk-resp. \ 
ui\browse.css
                                      C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
  Opens:
ui\button.css
                                      C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
  Opens:
ui\checkbox.css
                                      C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
  Opens:
ui\images
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\images\button-bg.png
                                      C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\images\progress-bg-corner.png
                                      C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
  Opens:
ui\images\progress-bg.png
                                      C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
  Opens:
ui\images\progress-bg2.png
                                      C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
  Opens:
ui\progress-bar.css
                                      C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279
  Opens:
                                      C:\Documents and Settings\Admin\Local
  Opens:
Settings\Temp\ish10855279\csshover3.htc
  Opens:
                                      C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\form.bmp.Mask
                                      C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\images
  Opens:
  Opens:
                                      C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\BG.png
                                      C:\Documents and Settings\Admin\Local
  Opens:
Settings\Temp\ish10855279\images\Close.png
                                      C:\Documents and Settings\Admin\Local
  Opens:
Settings\Temp\ish10855279\images\Close_Hover.png
  Opens:
                                      C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Color_Button.png
                                      C:\Documents and Settings\Admin\Local
  Opens:
Settings\Temp\ish10855279\images\Color_Button_Hover.png
                                      C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Grey_Button.png
  Opens:
                                      C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Grey_Button_Hover.png
                                      C:\Documents and Settings\Admin\Local
  Opens:
Settings\Temp\ish10855279\images\Icon_Generic.png
                                      C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Loader.gif
  Opens:
                                      C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Pause_Button.png
                                      C:\Documents and Settings\Admin\Local
  Opens:
Settings\Temp\ish10855279\images\Progress.png
  Opens:
                                      C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\ProgressBar.png
  Opens:
                                      C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Quick_Specs.png
                                      C:\Documents and Settings\Admin\Local
  Opens:
Settings\Temp\ish10855279\images\Resume_Button.png
                                      C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\locale
                                      C:\Documents and Settings\Admin\Local
  Opens:
Settings\Temp\ish10855279\locale\DE.locale
                                      C:\Documents and Settings\Admin\Local
  Opens:
Settings\Temp\ish10855279\locale\EN.locale
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\sdk
```

```
C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\ish10855279\sdk\exceptlist.txt
                         C:\WINDOWS\system32\iphlpapi.dll
 Opens:
                         C:\WINDOWS\system32\ws2_32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\ws2help.dll
 Opens:
                         C:\WINDOWS\system32\mprapi.dll
 Opens:
                         C:\WINDOWS\system32\activeds.dll
                         C:\WINDOWS\system32\adsldpc.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\netapi32.dll
 Opens:
                         C:\WINDOWS\system32\atl.dll
 Opens:
                         C:\WINDOWS\system32\rtutils.dll
 Opens:
                         C:\WINDOWS\system32\samlib.dll
 Opens:
                         C:\WINDOWS\system32\setupapi.dll
 Opens:
 Opens:
                         C:\Program Files\Internet Explorer
                         C:\Program Files\Internet Explorer\iexplore.exe
 Opens:
 Opens:
                         C:\WINDOWS\system32\clbcatq.dll
 Opens:
                         C:\WINDOWS\system32\comres.dll
 Opens:
                         C:\WINDOWS\Registration\R00000000007.clb
 Opens:
                         C:\WINDOWS\system32\ieframe.dll
 Opens:
                         C:\WINDOWS\system32\ieframe.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\ieframe.dll.123.Config
                         C:\WINDOWS\system32\en-US\ieframe.dll.mui
 Opens:
 Opens:
                         C:\WINDOWS\system32\sxs.dll
 Opens:
                         C:\WINDOWS\system32\MSIMTF.dll
                         C:\Documents and Settings
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings
 Opens:
                         C:\WINDOWS\system32\mlang.dll
                         C:\WINDOWS\system32\MLANG.dll.123.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\MLANG.dll.123.Config
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\bootstrap_3733.html
 Opens:
                         C:\WINDOWS\system32\mshtml.dll
 Opens:
                         C:\WINDOWS\system32\msls31.dll
 Opens:
                         C:\WINDOWS\system32\psapi.dll
 Opens:
                         C:\WINDOWS\system32\jscript.dll
 Opens:
                         C:\WINDOWS\system32\winlogon.exe
 Opens:
                         C:\WINDOWS\system32\xpsp2res.dll
 Opens:
                         C:\WINDOWS\system32\apphelp.dll
 Opens:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\ish10855279\sdk\ui\
 Opens:
                         {\tt C:\WINDOWS\AppPatch\symmin.sdb}
 Opens:
                         C:\WINDOWS\AppPatch\systest.sdb
 Opens:
                         C:\WINDOWS\Temp
                         C:\WINDOWS
 Opens:
 Opens:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\ish10855279\script\
 Opens:
                         C:\windows\temp\700aa61e9dbd14abfcc633546a5be910.exe.Manifest
 Opens:
                         C: \verb|\windows\temp\700aa61e9dbd14abfcc633546a5be910.exe.Config| \\
 Opens:
                         C:\WINDOWS\system32\iepeers.dll
 Opens:
                         C:\WINDOWS\system32\winspool.drv
                         C:\WINDOWS\system32\iepeers.dll.123.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\iepeers.dll.123.Config
 Opens:
                         C:\WINDOWS\system32\imgutil.dll
 Opens:
                         C:\WINDOWS\system32\pngfilt.dll
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5
                         C:\Documents and Settings\Admin\Local Settings\History
 Opens:
                         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
 Opens:
                         C:\Documents and Settings\Admin\Cookies
 Opens:
                         C:\Documents and Settings\Admin\Cookies\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\index.dat
                         C:\WINDOWS\Fonts\arialbd.ttf
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT
                         C:\WINDOWS\system32\powrprof.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\rasapi32.dll
 Opens:
                         C:\WINDOWS\system32\rasman.dll
                         C:\WINDOWS\system32\tapi32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\winmm.dll
 Opens:
                         C:\WINDOWS\system32\TAPI32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\TAPI32.dll.124.Config
 Opens:
                         C:\AUTOEXEC.BAT
                         C:\Documents and Settings\All Users\Application
 Opens:
{\tt Data\Microsoft\Network\Connections\Pbk}
                         C:\WINDOWS\system32\ras
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\Network\Connections\Pbk\
 Opens:
                         C:\WINDOWS\system32\sensapi.dll
                         C:\WINDOWS\svstem32\mswsock.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\rasadhlp.dll
```

```
Opens:
                                     C:\WINDOWS\system32\dnsapi.dll
                                     C:\Documents and Settings\Admin\Local Settings\Temp\00A69D39.log
  Opens:
  Opens:
                                     C:\WINDOWS\system32\drivers\etc\hosts
  Opens:
                                     C:\WINDOWS\system32\rsaenh.dll
  Opens:
                                     C:\WINDOWS\system32\msv1_0.dll
  Opens:
                                     C:\Documents and Settings\Admin\Local
Settings\Temp\ICReinstall_700aa61e9dbd14abfcc633546a5be910.exe
                                     C:\WINDOWS\system32\crypt32.dll
  Opens:
  Opens:
                                     C:\WINDOWS\system32\hnetcfg.dll
  Opens:
                                     C:\WINDOWS\system32\wshtcpip.dll
                                     C:\Documents and Settings\Admin\My Documents\desktop.ini
  Opens:
  Opens:
                                     C:\Documents and Settings\All Users
  Opens:
                                     C:\Documents and Settings\All Users\Documents\desktop.ini
  Opens:
                                     C:\WINDOWS\system32\linkinfo.dll
  Opens:
                                     C:\WINDOWS\system32\ntshrui.dll
  Opens:
                                     C:\WINDOWS\system32\ntshrui.dll.123.Manifest
  Opens:
                                     C:\WINDOWS\svstem32\ntshrui.dll.123.Config
  Opens:
                                     C:\Documents and Settings\Admin\Desktop
  Opens:
                                     C:\Documents and Settings\Admin\Start Menu\desktop.ini
  Opens:
                                     C:\Documents and Settings\All Users\Start Menu\desktop.ini
  Opens:
                                     C:\Documents and Settings\All Users\Application Data\desktop.ini
  Opens:
                                     C:\Documents and Settings\Admin\Application Data\desktop.ini
  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\msimg32.dll
  Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Temp\00A6A078.log
  Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Temp\is956058749
                                     C:\Documents and Settings\Admin\Local
  Opens:
Settings\Temp\is956058749\10920075_Setup.EXE
  Opens:
                                     C:\WINDOWS\system32\en-US\jscript.dll.mui
                                     C:\Documents and Settings\Admin\Local Settings\Temp\00A5A36F.log
  Writes to:
                                     C:\Documents and Settings\Admin\Local
  Writes to:
Settings\Temp\ish10855279\css\ie6_main.css
  Writes to:
                                     C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\css\main.css
                                     \label{thm:collinear} C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\ish10855279\css\sdk-resp. Temp\Admin\Local\ Settings\Temp\Barren \csp. Temp\Barren \csp. Temp\B
  Writes to:
ui\browse.css
                                     C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
  Writes to:
ui\button.css
                                     C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
  Writes to:
ui\checkbox.css
  Writes to:
                                     C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\images\button-bg.png
                                     C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\images\progress-bg-corner.png
  Writes to:
                                     C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\images\progress-bg.png
                                     C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
  Writes to:
ui\images\progress-bg2.png
                                     C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
  Writes to:
ui\progress-bar.css
  Writes to:
                                     C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\csshover3.htc
                                     C:\Documents and Settings\Admin\Local
  Writes to:
Settings\Temp\ish10855279\form.bmp.Mask
                                     C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\BG.png
                                     C:\Documents and Settings\Admin\Local
  Writes to:
Settings\Temp\ish10855279\images\Close.png
                                     C:\Documents and Settings\Admin\Local
  Writes to:
Settings\Temp\ish10855279\images\Close_Hover.png
                                     C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Color_Button.png
  Writes to:
                                     C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Color_Button_Hover.png
                                     C:\Documents and Settings\Admin\Local
  Writes to:
Settings\Temp\ish10855279\images\Grey_Button.png
  Writes to:
                                     C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Grey_Button_Hover.png
  Writes to:
                                     C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Icon_Generic.png
                                     C:\Documents and Settings\Admin\Local
  Writes to:
Settings\Temp\ish10855279\images\Loader.gif
  Writes to:
                                     C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Pause_Button.png
  Writes to:
                                     C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Progress.png
                                     C:\Documents and Settings\Admin\Local
  Writes to:
Settings\Temp\ish10855279\images\ProgressBar.png
```

```
Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Quick_Specs.png
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Resume_Button.png
                         C:\Documents and Settings\Admin\Local
 Writes to:
Settings\Temp\ish10855279\locale\DE.locale
                         C:\Documents and Settings\Admin\Local
 Writes to:
Settings\Temp\ish10855279\locale\EN.locale
                         C:\Documents and Settings\Admin\Local
 Writes to:
Settings\Temp\ish10855279\sdk\exceptlist.txt
                         C:\Documents and Settings\Admin\Local
 Writes to:
Settings\Temp\ish10855279\bootstrap_3733.html
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\00A69D39.log
                         C:\Documents and Settings\Admin\Local
 Writes to:
Settings\Temp\ICReinstall_700aa61e9dbd14abfcc633546a5be910.exe
 Writes to:
                         C:\Documents and Settings\Admin\Desktop\Continue CCleaner
Installation.lnk
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\00A6A078.log
 Reads from:
                         C:\WINDOWS\Temp\700aa61e9dbd14abfcc633546a5be910.exe
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\00A5A36F.log
 Reads from:
                         C:\WINDOWS\Registration\R00000000007.clb
 Reads from:
                         C:\WINDOWS\system32\ieframe.dll
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\ish10855279\bootstrap_3733.html
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\progress-bar.css
 Reads from:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\css\main.css
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\ish10855279\images\BG.png
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\ish10855279\images\Quick_Specs.png
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\ish10855279\locale\EN.locale
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\ish10855279\images\Grey_Button.png
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\ish10855279\images\Color_Button.png
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Close.png
                         {\tt C:\Documents\ and\ Settings\Admin\Local}
 Reads from:
Settings\Temp\ish10855279\images\Loader.gif
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\ish10855279\images\ProgressBar.png
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Progress.png
 Reads from:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Pause_Button.png
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\ish10855279\images\Resume_Button.png
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\ish10855279\form.bmp.Mask
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\ish10855279\images\Close_Hover.png
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\ish10855279\images\Grey_Button_Hover.png
 Reads from:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Color_Button_Hover.png
 Reads from:
                         C:\AUTOEXEC.BAT
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\00A69D39.log
 Reads from:
                         C:\WINDOWS\system32\drivers\etc\hosts
 Reads from:
                         C:\WINDOWS\system32\rsaenh.dll
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\ICReinstall_700aa61e9dbd14abfcc633546a5be910.exe
                         C:\Documents and Settings\Admin\My Documents\desktop.ini
 Reads from:
 Reads from:
                         C:\Documents and Settings\All Users\Documents\desktop.ini
 Reads from:
                         C:\Documents and Settings\Admin\Start Menu\desktop.ini
 Reads from:
                         C:\Documents and Settings\All Users\Start Menu\desktop.ini
 Reads from:
                         C:\Documents and Settings\All Users\Application Data\desktop.ini
                         C:\Documents and Settings\Admin\Application Data\desktop.ini
 Reads from:
 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
                         {\tt C:\Documents\ and\ Settings\ All\ Users\ Documents\ My\ Videos\ Desktop.ini}
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Icon_Generic.png
                         C:\Documents and Settings\Admin\Local Settings\Temp\00A6A078.log
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\00A5A36F.log
 Deletes:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\bootstrap_3733.html
                         C:\Documents and Settings\Admin\Local Settings\Temp\00A69D39.log
```

C:\Documents and Settings\Admin\Local Settings\Temp\00A6A078.log

Deletes:

Deletes:

Network Events

DNS query: os.softwarenetcdn.com DNS auerv: www.soft-ware.net

DNS response: os.softwarenetcdn.com \Rightarrow 54.77.202.184 DNS response: os.softwarenetcdn.com \Rightarrow 52.31.134.147 DNS response: os.softwarenetcdn.com \Rightarrow 54.194.194.239 DNS response: www.soft-ware.net \Rightarrow 104.27.164.7 www.soft-ware.net \Rightarrow 104.27.165.7 DNS response:

54.77.202.184:80 Connects to: Connects to: 104.27.164.7:80 Sends data to: 8.8.8.8:53

os.softwarenetcdn.com:80 (54.77.202.184) Sends data to: Sends data to: www.soft-ware.net:80 (104.27.164.7)

Receives data from: 0.0.0.0:0

Receives data from: os.softwarenetcdn.com:80 (54.77.202.184) Receives data from: www.soft-ware.net:80 (104.27.164.7)

Windows Registry Events

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

Creates key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints 2 \ \{f90255c2-6bc4-11e3-9fc7-16bc4-16bc$

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\tracing

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

folders

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

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

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

settings\connections

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

awareness

Creates kev: HKLM\svstem\currentcontrolset\services\tcpip\parameters Deletes value: HKCU\software\microsoft\windows\currentversion\internet

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

options\700aa61e9dbd14abfcc633546a5be910.exe

Opens key: HKLM\system\currentcontrolset\control\terminal server

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

options\gdi32.dll

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

options\user32.dll

Opens key: HKLM\system\currentcontrolset\control\session manager Opens key: HKLM\system\currentcontrolset\control\safeboot\option

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers

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

options\imm32.dll

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

options\ntdll.dll

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

options\kernel32.dll

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

options\secur32.dll Opens key:

HKLM\software\microsoft\windows nt\currentversion\image file execution options\rpcrt4.dll

Opens key: options\advapi32.dll

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

Opens key:

HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll

Opens key: options\ole32.dll HKLM\software\microsoft\windows nt\currentversion\image file execution

Opens key: options\oleaut32.dll HKLM\software\microsoft\windows nt\currentversion\image file execution HKLM\software\microsoft\windows nt\currentversion\image file execution

Opens kev: options\comctl32.dll

Opens key: HKLM\system\currentcontrolset\control\error message instrument\ Opens kev: HKLM\svstem\currentcontrolset\control\error message instrument Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32

Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility Opens key: HKLM\software\microsoft\windows nt\currentversion\windows Opens key: $\label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + nt + current + version + winlog on + current + version + version$

Opens key: HKLM\

Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics Opens key: HKLM\software\microsoft\ole

Opens key: HKCR\interface

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

Opens key: HKLM\software\microsoft\oleaut

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

Opens key: HKCU\

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

Opens key: HKCU\control panel\desktop

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

options\shlwapi.dll

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

options\shell32.dll

Opens key: HKLM\system\setup

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\windows nt\currentversion\image file execution

options\comdlg32.dll

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

options\iertutil.dll

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

options\urlmon.dll

Opens key: HKCU\software\classes\

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

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

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

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

settings\

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

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

Opens key: HKCU\software\microsoft\internet

 $explorer \verb|\main| featurecontrol| feature_ignore_policies_zonemap_if_esc_enabled_kb918915$

Opens key: HKLM\software\microsoft\internet

 $\label{lem:control} explorer $$ explorer \rightarrow \frac{1}{esc_{enabled_kb918915}} $$ Opens key: $$ HKLM \circ \frac{1}{esc_{enabled_kb918915}} $$ explorer \rightarrow \frac{1}{esc_{enabled_kb918915}} $$ Opens key: $$ HKLM \circ \frac{1}{esc_{enabled_kb918915}} $$ explorer \rightarrow \frac{1}{esc_{enabled_kb918915}} $$ Opens key: $$ HKLM \circ \frac{1}{esc_{enabled_kb918915}} $$ explorer \rightarrow \frac{1}{esc_{enabled_kb918915}} $$ expl$

settings\zonemap\domains\

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

settings\zonemap\domains\

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

settings\zonemap\ranges\

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

settings\zonemap\ranges\

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

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

options\version.dll

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

options\normaliz.dll

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

options\wininet.dll

Opens key: HKLM\system\currentcontrolset\control\wmi\security

Opens key: HKCU\software\borland\locales
Opens key: HKLM\software\borland\locales
Opens key: HKCU\software\borland\delphi\locales

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

options\olepro32.dll

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

options\msctf.dll

Opens key:

HKLM\software\microsoft\ctf\compatibility\700aa61e9dbd14abfcc633546a5be910.exe

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

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

Opens key: ${\tt HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current \vee ersion \setminus imm}$

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

options\msctfime.ime

Opens key: HKCU\software\microsoft\ctf

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

Opens key: HKLM\software\microsoft\rpc

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

options\700aa61e9dbd14abfcc633546a5be910.exe\rpcthreadpoolthrottle Opens key: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKLM\system\currentcontrolset\control\computername

HKLM\system\currentcontrolset\control\computername\activecomputername Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\ws2help.dll

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

options\ws2_32.dll

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

options\iphlpapi.dll

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

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

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

Opens key:

c7d49d7cecdc}

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

options\netapi32.dll

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

options\wldap32.dll

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

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

options\adsldpc.dll

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

options\atl.dll

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

options\activeds.dll

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

options\rtutils.dll

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

options\samlib.dll

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

 ${\tt HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus setup}$ Opens key: Opens key: ${\it HKLM \ } software \ \\ microsoft \ \\ windows \ \\ current version$

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

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

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

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

options\mprapi.dll

Opens key:

HKCU\software\microsoft\windows\shell\associations\urlassociations\http\userchoice

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

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

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} in the constraint of the cons$ Opens key:

Opens key: HKLM\software\microsoft\com3 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\comres.dll

Opens key:

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

options\clbcatq.dll

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

HKLM\software\classes Opens key:

Opens key: HKU∖

Opens key: HKCR\clsid

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

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

00c04fd705a2}\treatas

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

00c04fd705a2}\inprocserver32

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

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

00c04fd705a2}\inprocserverx86

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

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

00c04fd705a2}\localserver32

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

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

00c04fd705a2}\inprochandler32

 $HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\tinprochandler 32$ Opens key:

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

00c04fd705a2}\inprochandlerx86

Opens key:

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

00c04fd705a2}\localserver

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

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

options\ieframe.dll

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

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

0000c05bae0b}\typelib

 $HKCR\interface \\ \{eab22ac1-30c1-11cf-a7eb-0000c05bae0b\} \\ typelib$ Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba} Opens key:

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

00aa00404770}\proxystubclsid32

Opens key:

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

00aa004ba90b}\proxystubclsid32

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

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

00000000046}\proxystubclsid32

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

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

00c04f79abd1}\proxystubclsid32

Opens key: $HKCR \ log \ 493f2f68c-1d1b-11d3-a30e-00c04f79abd1 \ \ proxystubclsid32$ Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\sxs.dll

Opens key: HKCU\software\classes\typelib

Opens key: HKCR\typelib

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

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

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

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

0000c05bae0b}\1.1\0

HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0 Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus typelib \setminus \{eab 22ac 0 - 30c 1 - 11cf - a7eb - a7e$

0000c05bae0b}\1.1\0\win32

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

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

settings\zonemap\

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001

HKLM\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001

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

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

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

settings\zonemap\ranges\

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

settings\zonemap\protocoldefaults\

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

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

settings\zonemap\domains\

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

settings\zonemap\domains\msn.com

Opens key:

HKLM\software\microsoft\windows\currentversion\internet settings\zonemap\domains\msn.com\related

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: 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: $\label{lem:hkcu} \mbox{\current} windows \mbox{\current} internet settings \mbox{\current} settings \mbox{\current} and \mbo$ Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4

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

settings\zones\

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

Opens key:

 $\label{lem:hklmsoftware policies microsoft windows \current version \cite{thmsoftware} in the lemma of the$

settings\zones\0

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

settings\zones\0

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

settings\zones\1

Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}$

settings\zones\1

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

```
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
 Opens key:
                        \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
settings\zones\3
                        HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\4
 Opens key:
                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
 Opens key:
                        \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\
                        HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\
 Opens key:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\
 Opens key:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                        HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\0
                        HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\0
 Opens key:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                        HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\1
                        HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\1
 Opens key:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
                        HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\2
 Opens key:
                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
                        HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\3
                        HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\3
 Opens key:
                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                        HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\4
                        HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\4
                        HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\4
 Opens key:
                        HKCR\clsid\{3050f4e1-98b5-11cf-bb82-00aa00bdce0b}
                        HKCR\clsid\{3050f4f5-98b5-11cf-bb82-00aa00bdce0b}
 Opens key:
                        HKCR\clsid\{3050f819-98b5-11cf-bb82-00aa00bdce0b}
 Opens key:
 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\microsoft\windows\currentversion\policies\explorer
 Opens key:
                        HKCU\software\microsoft\windows\currentversion\policies\explorer
 Opens key:
Opens kev:
a2d8-08002b30309d}
 Opens key:
                        HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32
 Opens key:
                        HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32
 Opens kev:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume
11e3-9fc7-806d6172696f}\
 Opens key:
                        HKCU\software\classes\drive\shellex\folderextensions
 Opens kev:
                        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
                        HKCR\directory
 Opens kev:
 Opens key:
                        HKCU\software\classes\directory\curver
```

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

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

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

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

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

Opens key: HKCR\folder

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

Opens key: HKCR\folder\clsid

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

Opens key: HKCU\software\classes\.html

Opens key: HKCR\.html

Opens key: HKCU\software\classes\htmlfile

Opens key: HKCR\htmlfile

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

Opens key: HKCR\htmlfile\curver Opens key: HKCR\htmlfile\

HKCU\software\classes\htmlfile\shellex\iconhandler Opens kev:

Opens key: HKCR\htmlfile\shellex\iconhandler

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

Opens key: HKCR\systemfileassociations\.html

Opens key: HKCU\software\classes\systemfileassociations\text

Opens key: HKCR\systemfileassociations\text HKCU\software\classes\htmlfile\clsid Opens key:

Opens key: HKCR\htmlfile\clsid

Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\implemented categories\{00021490-0000-0000-c000-000000000046}

Opens key:

categories\{00021490-0000-0000-c000-00000000046}

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: HKCU\software\classes\htmlfile\shellex\{a39ee748-6a27-4817-a6f2-

13914bef5890}

Opens key: HKCR\htmlfile\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890} Opens key: HKCU\software\classes\.html\shellex\{a39ee748-6a27-4817-a6f2-

13914bef5890}

HKCR\.html\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890} Opens key:

Opens key: $HKCU \setminus software \setminus classes \setminus system file associations \setminus text \setminus shellex \setminus \{a39ee748-text\} = \{a39ee748-$

6a27-4817-a6f2-13914bef5890}

 $HKCR \ system file associations \ text \ shellex \ \ \{a39ee748-6a27-4817-a6f2-4817-a$ Opens key:

13914bef5890}

HKCU\software\classes* Opens kev:

HKCR* Opens key:

Opens key: $HKCU \setminus software \setminus classes \setminus * \setminus shellex \setminus \{a39ee748-6a27-4817-a6f2-13914bef5890\}$

Opens key: HKCR*\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615 Opens key: HKCU\software\microsoft\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_iedde_register_protocol Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_iedde_register_protocol

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

00000000046}

Opens key: HKCR\htmlfile\shellex\{000214e6-0000-0000-c000-00000000046} Opens key: HKCU\software\classes\.html\shellex\{000214e6-0000-0000-c000-

000000000046}

Opens key: HKCR\.html\shellex\{000214e6-0000-0000-c000-00000000046}

Opens key: $HKCU \setminus software \setminus classes \setminus system file associations \setminus text \setminus shellex \setminus \{000214e6-text\} \cap system file associations \setminus text \setminus shellex \setminus \{000214e6-text\} \cap system file associations \setminus text \setminus shellex \setminus \{000214e6-text\} \cap system file associations \setminus text \setminus shellex \setminus \{000214e6-text\} \cap system file associations \setminus text \setminus shellex \setminus \{000214e6-text\} \cap system file associations \setminus text \setminus shellex \setminus \{000214e6-text\} \cap system file associations \setminus text \setminus shellex \setminus \{000214e6-text\} \cap system file associations \setminus text \setminus shellex \setminus \{000214e6-text\} \cap system file associations \setminus text \setminus shellex \setminus \{000214e6-text\} \cap system file associations \setminus text \setminus shellex \setminus \{000214e6-text\} \cap system file associations \setminus text \setminus shellex \setminus \{000214e6-text\} \cap system file associations \cap system file association file associations \cap system file association file associations \cap syst$

0000-0000-c000-000000000046}

Opens key:

000000000046}

HKCU\software\classes*\shellex\{000214e6-0000-0000-c000-000000000046} Opens key:

Opens key: HKCR*\shellex\{000214e6-0000-0000-c000-00000000046}

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

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

settings\accepted documents

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

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000

```
HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature zones default drive intranet kb941000
 Opens key:
                         HKCU\software\microsoft\internet explorer
                         HKLM\software\microsoft\internet explorer
 Opens key:
 Opens kev:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_mime_handling
 Opens key:
                         HKCU\software\classes\protocols\name-space handler\file\
                         HKCR\protocols\name-space handler\file
 Opens key:
 Opens key:
                         HKCU\software\classes\protocols\name-space handler\*\
 Opens key:
                         HKCR\protocols\name-space handler\*
 Opens key:
                         HKCU\software\classes\protocols\filter\text/html
                         HKCR\protocols\filter\text/html
 Opens kev:
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_mime_sniffing
 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\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
 Opens kev:
 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
 Opens key:
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserverx86
 Opens key:
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserverx86
 Opens key:
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\localserver32
 Opens key:
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\localserver32
 Opens key:
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprochandler32
 Opens key:
                         \label{lem:hkcrclsid} $$HKCR\clsid_{25336920-03f9-11cf-8fd0-00aa00686f13}\in All $$\clsid_{25336920-03f9-11cf-8fd0-00aa00686f13}$$
 Opens key:
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprochandlerx86
 Opens key:
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandlerx86
 Opens key:
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\localserver
 Opens key:
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\localserver
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msls31.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mshtml.dll
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
                         HKCU\software\microsoft\internet
 Opens key:
Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_aria_support
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_aria_support
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams
                         HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_legacy_dispparams
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_private_font_setting
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_private_font_setting
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_css_show_hide_events
                         HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature css show hide events
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_allow_expanduri_bypass
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_expanduri_bypass
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
```

```
HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
 Opens kev:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
 Opens kev:
                         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 kev:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
                         HKLM\software\microsoft\internet
 Opens key:
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 kev:
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
 Opens key:
                         HKCU\software\microsoft\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
                         HKLM\software\microsoft\windows\currentversion\app paths\outlook.exe
 Opens key:
 Opens key:
                         {\tt HKLM \setminus software \setminus microsoft \setminus internet\ explorer \setminus application\ compatibility}
 Opens key:
                         HKLM\software\policies\microsoft\internet explorer\domstorage
                         HKCU\software\policies\microsoft\internet explorer\domstorage
 Opens key:
 Opens key:
                         HKCU\software\microsoft\internet explorer\domstorage
 Opens key:
                         HKLM\software\microsoft\internet explorer\domstorage
                         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 key:
                         HKLM\software\microsoft\internet explorer\safety\privacie
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\psapi.dll
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_manage_script_circular_refs
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_manage_script_circular_refs
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_restrict_filedownload
 Opens key:
                         HKLM\software\microsoft\internet explorer\security\floppy access
                         HKCU\software\microsoft\internet explorer\security\adv addrbar spoof
 Opens key:
detection
 Opens kev:
                         HKLM\software\microsoft\internet explorer\security\adv addrbar spoof
detection
                         HKCU\software\classes\protocols\name-space handler\about\
 Opens key:
 Opens key:
                         HKCR\protocols\name-space handler\about
                         HKCU\software\classes\protocols\handler\about
 Opens key:
 Opens key:
                         HKCR\protocols\handler\about
                         HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
 Opens key:
                         HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
 Opens key:
 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 \c1sid \c13050f406-98b5-11cf-bb82-00aa00bdce0b\c1inprocserver32
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserverx86
                         HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\localserver32
                         HKCR \clsid \ \{3050f406-98b5-11cf-bb82-00aa00bdce0b\} \localserver 32
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
                         HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\ \ inprochandler 32
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandlerx86
                         HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\localserver
```

 $HKCR \verb|\clsid|{3050f406-98b5-11cf-bb82-00aa00bdce0b}\\ \\localserver$

Opens key:

```
HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_document_compatible_mode
 Opens kev:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_document_compatible_mode
 Opens kev:
                         HKLM\software\microsoft\windows\currentversion\internet settings\zones\3
 Opens key:
                         HKLM\software\policies\microsoft\internet explorer\zoom
 Opens key:
                         HKCU\software\policies\microsoft\internet explorer\zoom
                         HKCU\software\microsoft\internet explorer\zoom
 Opens key:
 Opens key:
                         HKLM\software\microsoft\internet explorer\zoom
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_weboc_document_zoom
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_weboc_document_zoom
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
 Opens key:
00aa00686f13}\progid
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid
 Opens key:
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_enable_compat_logging
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_compat_logging
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dlcontrol_behaviors
                         HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_legacy_dlcontrol_behaviors
 Opens key:
                         HKCU\software\policies\microsoft\internet explorer
                         HKLM\software\policies\microsoft\internet explorer\international\scripts
 Opens key:
 Opens key:
                         HKCU\software\microsoft\internet explorer\international\scripts
                         HKLM\software\microsoft\internet explorer\international\scripts
 Opens key:
                         HKLM\software\policies\microsoft\internet explorer\settings
 Opens kev:
 Opens key:
                         HKCU\software\microsoft\internet explorer\settings
 Opens key:
                         HKLM\software\microsoft\internet explorer\settings
 Opens key:
                         HKCU\software\microsoft\internet explorer\styles
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\policies\activedesktop
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\policies
 Opens key:
                         HKCU\software\microsoft\internet explorer\pagesetup
 Opens key:
                         HKCU\software\microsoft\internet explorer\menuext
 Opens key:
                         HKCU\software\microsoft\internet explorer\menuext\%s
                         HKLM\system\currentcontrolset\control\nls\codepage
 Opens key:
 Opens key:
                         HKCU\software\microsoft\internet explorer\international\scripts\3
```

HKCU\software\microsoft\windows\currentversion\explorer\travellog
HKLM\software\microsoft\windows\currentversion\explorer\travellog

HKLM\software\microsoft\windows\currentversion\internet settings\zones\0

HKCU\software\microsoft\windows\currentversion\internet settings\zones

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

HKCU\software\microsoft\windows\currentversion\internet settings\

HKLM\software\microsoft\windows\currentversion\internet settings\

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

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

HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}

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

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

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

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

 $\label{local-HKCR} $HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc} \land HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc} \land HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc} \land HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc} \land HKCU\software\classes\clsid\cls$

 $HKCU \setminus software \setminus classes \setminus clsid \setminus \{50d5107a - d278 - 4871 - 8989 - d278 - d$

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

 $HKCU \setminus software \setminus classes \setminus clsid \setminus \{50d5107a - d278 - 4871 - 8989 - d278 - d$

HKLM\software\microsoft\internet explorer\version vector

HKCU\software\microsoft\internet

HKLM\software\microsoft\internet

HKCU\software\microsoft\internet

HKLM\software\microsoft\internet

HKCU\software\microsoft\internet

HKLM\software\microsoft\internet

HKCU\software\microsoft\internet

HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_zone_elevation

explorer\main\featurecontrol\feature_zone_elevation

explorer\main\featurecontrol\feature browser emulation

explorer\main\featurecontrol\feature_browser_emulation

explorer\main\featurecontrol\feature_sslux

explorer\main\featurecontrol\feature_sslux

explorer\main\featurecontrol\feature_xssfilter

explorer\main\featurecontrol\feature_xssfilter

Opens key:

Opens key: Opens key:

Opens key:

Opens kev:

Opens key:

Opens kev:

Opens key:

Opens key:

Opens kev:

Opens key:

Opens key: Opens key:

Opens key:

Opens key:

Opens key: Opens key:

settings\zonemap\
Opens key:

settings\zonemap\ Opens key:

f4ceaaf59cfc}\treatas

f4ceaaf59cfc}\inprocserver32

f4ceaaf59cfc}\inprocserverx86

f4ceaaf59cfc}\localserver32

settings\ Opens key:

```
f4ceaaf59cfc}\inprochandler32
                                                                                                                     HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandler32
       Opens kev:
       Opens key:
                                                                                                                     HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprochandlerx86
       Opens kev:
                                                                                                                     HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandlerx86
       Opens key:
                                                                                                                     HKCU \setminus software \setminus classes \setminus clsid \setminus \{50d5107a - d278 - 4871 - 8989 - d278 - d
f4ceaaf59cfc}\localserver
       Opens key:
                                                                                                                    HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\localserver
       Opens key:
                                                                                                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msimtf.dll
       Opens kev:
                                                                                                                     HKLM\software\microsoft\ctf\tip
       Opens key:
                                                                                                                     HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
c9633f71be64}\languageprofile
                                                                                                                    HKCU\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
       Opens key:
c9633f71be64}\languageprofile
       Opens key:
                                                                                                                     HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\languageprofile\0x00000000
       Opens key:
                                                                                                                     HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}
                                                                                                                    \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \classes \clsid \ \{3ce74de4-53d3-4d74-8b83-431b3828ba53\} \end{tabular}
       Opens key:
       Opens key:
                                                                                                                     HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}
       Opens key:
                                                                                                                     HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\treatas
       Opens key:
                                                                                                                     HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\treatas
       Opens key:
                                                                                                                     HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprocserver32
                                                                                                                     HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32
       Opens key:
       Opens key:
                                                                                                                     HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprocserverx86
       Opens key:
                                                                                                                     HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserverx86
       Opens key:
                                                                                                                     HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\localserver32
                                                                                                                     HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver32
       Opens key:
       Opens key:
                                                                                                                     HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprochandler32
       Opens key:
                                                                                                                     HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandler32
       Opens key:
                                                                                                                     HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprochandlerx86
                                                                                                                     HKCR \c1sid \c2seq4de4-53d3-4d74-8b83-431b3828ba53 \c2seq4de4-53d3-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-4d74-8b83-8d74-8b83-8d74-8b83-8d74-8b83-8d74-8b83-8d74-8b83-8d74-8
       Opens key:
       Opens key:
                                                                                                                     HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\localserver
       Opens key:
                                                                                                                     HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver
                                                                                                                     HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}
       Opens kev:
                                                                                                                     HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}
       Opens key:
                                                                                                                     HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
       Opens key:
869523e2d6c7}\treatas
                                                                                                                     HKCR\clsid{a4b544a1-438d-4b41-9325-869523e2d6c7}\treatas
       Opens key:
       Opens key:
                                                                                                                     869523e2d6c7}\inprocserver32
                                                                                                                    HKCR \c1sid \a4b544a1-438d-4b41-9325-869523e2d6c7 \c1sid \a4b544a1-438d-4b41-9325-869523e2d6c7 \c1sid \c1
       Opens key:
                                                                                                                     HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
       Opens kev:
869523e2d6c7}\inprocserverx86
                                                                                                                     HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserverx86
       Opens key:
                                                                                                                     HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
       Opens key:
869523e2d6c7}\localserver32
                                                                                                                    HKCR \ clsid \ \{a4b544a1-438d-4b41-9325-869523e2d6c7\} \ localserver 32
       Opens key:
                                                                                                                     HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
       Opens key:
869523e2d6c7}\inprochandler32
                                                                                                                     HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandler32
       Opens key:
       Opens key:
                                                                                                                     HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprochandlerx86
       Opens key:
                                                                                                                    HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandlerx86
                                                                                                                     HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
       Opens key:
869523e2d6c7}\localserver
                                                                                                                    HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\localserver
       Opens key:
       Opens key:
                                                                                                                     HKLM\software\microsoft\ctf\tip\
       Opens key:
                                                                                                                     HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
{\tt c9633f71be64} \\ {\tt category} \\ {\tt b95f181b-ea4c-4af1-8056-7c321abbb091} \\ {\tt c9633f71be64} \\ {\tt category} \\ {
       Opens key:
                                                                                                                     HKLM \setminus software \setminus microsoft \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-4fc
77e8f3d1aa80}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
       Opens key:
                                                                                                                     HKLM \setminus software \setminus icrosoft \setminus tip \setminus \{c1ee01f2-b3b6-4a6a-9ddd-b4b4\} = \{c1ee01f2-b3b6-4a6a-9ddb-b4b4\} = \{c1ee01f2-b3b6-4a6a-9db-b4b4\} = \{c1ee01f2-b3b6-4a6a-9db-b4b4\} = \{c1ee01f2-b3b6-4a6a-9db-b4b4\} = \{c1ee01f2-b3b6-4a6a-9db-b4b4\} = \{c1ee01f2-b3b6-4a6a-6ab4\} = \{c1ee01f2-b3b6-4a6a-6ab4\} = \{c1ee01f2-b3b6-4a6a-6ab4\} = \{c1ee01f2-b3b6-4a6a-6ab4\} = \{c1ee01f2-b3b6-4a6a-6ab4\} = \{c1ee01f2-b3b6-4a6a-6ab4\} = \{c1ee01f2-b4b6-4a6a-6ab4\} = \{c1e
e988c088ec82}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
                                                                                                                    HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
      Opens kev:
00c04fc324a1}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
       Opens key:
                                                                                                                     HKLM \setminus software \setminus microsoft \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-bd2
Of816c09f4ee}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
       Opens key:
                                                                                                                     HKCU\software\microsoft\ctf\langbaraddin\
                                                                                                                     HKLM\software\microsoft\ctf\langbaraddin\
       Opens kev:
       Opens key:
                                                                                                                     HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
```

HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-

 $HKLM \setminus software \setminus microsoft \setminus tip \setminus \{c1ee01f2-b3b6-4a6a-9ddd-based \} = \{c1ee01f2-b3b6-4a6a-9ddb-based \} = \{c1ee01f2-b3b6-4a6a-9db-based \} = \{c1ee01f2-b3b6-4a6a-9db-based \} = \{c1ee01f2-b3b6-4a6a-9db-based \} = \{c1ee01f2-b3b6-4a6a-9db-based \} = \{c1ee01f2-b3b6-4a$

77e8f3d1aa80}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}

Opens key:

Opens key:

```
e988c088ec82}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
                                                        HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
   Opens key:
00c04fc324a1}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
                                                        HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-
   Opens key:
Of816c09f4ee}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
   Opens key:
                                                        HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
c9633f71be64}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
                                                        HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
   Opens key:
77e8f3d1aa80\} \\ category \\ item \\ \{5130a009-5540-4fcf-97eb-aad33fc0ee09\} \\
                                                        Opens key:
c9633f71be64}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
   Opens key:
                                                        HKLM \setminus software \setminus microsoft \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-4fc
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
                                                        HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
   Opens key:
c9633f71be64\\ \\ category\\ \\ item\\ \\ c6debc0a-f2b2-4f17-930e-ca9faff4cd04\\ \\ \\
   Opens key:
                                                        HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80\} \land (c6debc0a-f2b2-4f17-930e-ca9faff4cd04)
   Opens key:
                                                        HKCU\software\policies\microsoft\internet explorer\control panel
   Opens key:
                                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
   Opens key:
                                                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
                                                        HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
   Opens kev:
   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
   Opens key:
                                                        HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserverx86
   Opens key:
                                                        HKCR\clsid\f414c260-6ac0-11cf-b6d1-00aa00bbbb58\\\linerocserverx86
   Opens key:
                                                        HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\localserver32
   Opens key:
                                                        HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\localserver32
   Opens key:
                                                        HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprochandler32
   Opens key:
                                                        HKCR\clsid\f414c260-6ac0-11cf-b6d1-00aa00bbbb58\\\inprochandler32
   Opens key:
                                                        HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprochandlerx86
   Opens key:
                                                        HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprochandlerx86
   Opens key:
                                                        HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\localserver
   Opens key:
                                                        HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\localserver
   Opens key:
                                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\jscript.dll
   Opens key:
                                                        HKLM\software\microsoft\windows script\features
   Opens key:
                                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547
                                                        HKLM\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547
                                                        {\tt HKLM \backslash software \backslash microsoft \backslash internet\ explorer \backslash activex\ compatibility}
   Opens key:
   Opens key:
                                                        HKLM\software\microsoft\internet explorer\activex
compatibility\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
                                                        HKLM\system\currentcontrolset\control\nls\locale
   Opens key:
   Opens key:
                                                        HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
                                                        HKLM\system\currentcontrolset\control\nls\language groups
   Opens key:
   Opens key:
                                                        HKCU\software\classes\appid\700aa61e9dbd14abfcc633546a5be910.exe
   Opens key:
                                                        HKCR\appid\700aa61e9dbd14abfcc633546a5be910.exe
   Opens key:
                                                        HKLM\system\currentcontrolset\control\lsa
   Opens key:
                                                        history
   Opens key:
                                                        HKCU\software\microsoft\ftp
                                                        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
                                                        HKLM\software\policies\microsoft\internet explorer\activities
   Opens key:
   Opens key:
                                                        HKCU\software\microsoft\internet explorer\activities
   Opens key:
                                                        HKLM\software\microsoft\internet explorer\activities
   Opens key:
                                                        HKLM\software\policies\microsoft\internet
explorer\infodelivery\restrictions
   Opens key:
                                                        HKCU\software\policies\microsoft\internet
explorer\infodelivery\restrictions
   Opens key:
                                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_binary_caller_service_provider
   Opens key:
                                                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_binary_caller_service_provider
   Opens key:
                                                        HKLM\software\policies\microsoft\internet explorer\restrictions
   Opens kev:
                                                        HKCU\software\policies\microsoft\internet explorer\restrictions
   Opens key:
                                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_additional_ie8_memory_cleanup
   Opens key:
                                                        HKLM\software\microsoft\internet
```

explorer\main\featurecontrol\feature_additional_ie8_memory_cleanup Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\apphelp.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\xpsp2res.dll HKLM\svstem\wpa\tabletpc Opens key: Opens key: HKLM\system\wpa\mediacenter HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers Opens key: Opens kev: HKLM\software\microsoft\windows $nt \verb|\currentversion| app compatflags \verb|\custom|| 700 aa 61 e 9 db d 14 ab f cc 633546 a 5 be 910. executive for the contraction of the contract$ Opens key: HKLM\software\policies\microsoft\windows\safer\levelobjects Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths Opens key: he2efd2c1a33} Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes Opens key: edd5fbde1328} Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert Opens key: b813f72dbb91} HKCU\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_ignore_leading_file_separator_in_uri_kb933105 HKLM\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_ignore_leading_file_separator_in_uri_kb933105 HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_subdownload_lockdown Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f} Opens key: 085bcc18a68d} HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_subdownload_lockdown Opens kev: b91490411bfc} Opens key: HKCU\software\classes\.css Opens key: HKCR\.css Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561 Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths Opens key: $HKLM \ software \ bolicies \ microsoft \ windows \ safer \ code identifiers \ 65536 \ has hes$ Opens kev: $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus urlzones$ HKLM\software\policies\microsoft\internet explorer\dxtrans Opens kev: Opens key: HKCU\software\microsoft\internet explorer\dxtrans Opens key: $\label{lem:hklm} \mbox{HKLM} \mbox{$\mbox{hklm}\end{\mbox{$\mbox{$\mbox{$ware}$} irrosoft\end{\mbox{$\mbox{}\mbox{\mbo Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths Opens kev:

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

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

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

Opens key:

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

Opens key:

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

Opens key:

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

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation

Opens key:

 $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus hashes$

Opens kev:

Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths

Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes

Opens key:

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

Opens key:

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

Opens key:

Opens key:

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

Opens key:

 $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus paths$

Opens key: HKLM\software\microsoft\internet explorer\default behaviors

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

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

00aa00bdce0b}\treatas

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

Opens key:

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

Opens key:

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

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

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

00aa00bdce0b}\inprocserver32

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

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

00aa00bdce0b}\inprocserverx86

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

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

00aa00bdce0b}\localserver32

 $Opens~key: \\ HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\localserver32$

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

00aa00bdce0b}\inprochandler32

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

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

00aa00bdce0b}\inprochandlerx86

 $Opens~key: \\ HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\ \ inprochandler x86 \\$

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

00aa00bdce0b}\localserver

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

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

options\winspool.drv

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

options\iepeers.dll

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

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_scripturl_mitigation Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_scripturl_mitigation Opens key: HKCU\software\classes\.png

Opens key: HKCR\.png

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

options\imgutil.dll

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

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

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

00aa006c1a01}\treatas

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

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

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 kev: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandlerx86 Opens key: 00aa006c1a01}\localserver HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver Opens key: Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01} HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01} Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-Opens key: 00aa006c1a01}\treatas Opens key: $HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01\}\treatas$ HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-Opens key: 00aa006c1a01}\inprocserver32 HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32 Opens key: Opens kev: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserverx86 Opens key: $HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01\}\inprocserverx86$ Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver32 HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver32 Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-Opens kev: 00aa006c1a01}\inprochandler32 Opens key: $HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01\}\inprochandler 32$ Opens key: 00aa006c1a01}\inprochandlerx86 Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandlerx86 HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-Opens kev: 00aa006c1a01}\localserver Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver HKCU\software\classes\mime\database\content type Opens key: Opens key: HKCR\mime\database\content type Opens key: HKCU\software\classes\mime\database\content type\image/bmp\bits HKCR\mime\database\content type\image/bmp\bits Opens key: HKCU\software\classes\mime\database\content type\image/gif\bits Opens key: Opens key: HKCR\mime\database\content type\image/gif\bits $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \mime \database \content type \simple \mime \database \content type \simple \mime \mime$ Opens key: Opens key: HKCR\mime\database\content type\image/jpeg\bits Opens key: HKCU\software\classes\mime\database\content type\image/pjpeg\bits Opens key: HKCR\mime\database\content type\image/pjpeg\bits Opens key: HKCU\software\classes\mime\database\content type\image/png\bits Opens kev: HKCR\mime\database\content type\image/png\bits Opens key: HKCU\software\classes\mime\database\content type\image/tiff\bits Opens key: HKCR\mime\database\content type\image/tiff\bits Opens key: HKCU\software\classes\mime\database\content type\image/x-icon\bits Opens key: HKCR\mime\database\content type\image/x-icon\bits Opens key: HKCU\software\classes\mime\database\content type\image/x-jg\bits Opens kev: HKCR\mime\database\content type\image/x-jg\bits Opens key: HKCU\software\classes\mime\database\content type\image/x-png\bits Opens kev: HKCR\mime\database\content type\image/x-png\bits HKCU\software\classes\mime\database\content type\image/x-wmf\bits Opens key: Opens key: HKCR\mime\database\content type\image/x-wmf\bits Opens key: HKCU\software\classes\mime\database\content type\image/x-png Opens kev: HKCR\mime\database\content type\image/x-png $HKCU \setminus software \setminus classes \setminus clsid \setminus \{a3ccedf7-2de2-11d0-86f4-00a0c913f750\}$ Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750} Opens key: Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\treatas Opens key: $HKCR\clsid\a3ccedf7-2de2-11d0-86f4-00a0c913f750$ \treatas Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32 HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32

Opens key:

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

00a0c913f750}\inprocserverx86

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

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

00a0c913f750}\localserver32

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

00a0c913f750}\inprochandler32 Opens kev:

HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandler32 Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-

00a0c913f750}\inprochandlerx86

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

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

00a0c913f750}\localserver

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

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

options\pngfilt.dll

Opens key: HKCU\software\classes\.gif

Opens kev: HKCR\.gif

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

```
settings\5.0\cache
                                                                      HKCU\software\microsoft\windows\currentversion\internet
    Opens key:
 settings\5.0\cache
     Opens key:
                                                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
    Opens key:
                                                                      HKLM\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\content
                                                                     \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
    Opens key:
 settings\5.0\cache\cookies
                                                                     HKLM\software\microsoft\windows\currentversion\internet
     Opens key:
settings\5.0\cache\cookies
     Opens key:
                                                                      \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} in the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu
 settings\5.0\cache\history
                                                                     HKLM\software\microsoft\windows\currentversion\internet
    Opens key:
 settings\5.0\cache\history
     Opens key:
                                                                      HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache
     Opens key:
                                                                     HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\domstore
                                                                     HKCU\software\microsoft\windows\currentversion\internet
    Opens key:
 settings\5.0\cache\extensible cache\feedplat
                                                                      HKCU\software\microsoft\windows\currentversion\internet
    Opens key:
 settings\5.0\cache\extensible cache\iecompat
     Opens key:
                                                                      HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\ietld
                                                                     HKCU\software\microsoft\windows\currentversion\internet
    Opens key:
 settings\5.0\cache\extensible cache\mshist012014033120140407
                                                                     HKCU\software\microsoft\windows\currentversion\internet
    Opens key:
 settings\5.0\cache\extensible cache\mshist012014041220140413
                                                                      HKCU\software\microsoft\windows\currentversion\internet
     Opens key:
 settings\5.0\cache\extensible cache\privacie:
                                                                     HKLM \setminus software \setminus microsoft \setminus ctf \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 80
    Opens key:
 c9633f71be64}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
     Opens key:
                                                                      HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80\} \\ category \\ item \\ \{a48fa74e-f767-44e4-bfbc-169e8b38ff58\} \\
                                                                      HKLM \setminus software \setminus microsoft \setminus tip \setminus \{c1ee01f2-b3b6-4a6a-9ddd-based \mid the first of the first of
     Opens key:
e988c088ec82}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                                                                     Opens key:
00c04fc324a1}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                                                                     HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-}
     Opens key:
HKCU\software\microsoft\internet
     Opens key:
explorer\main\featurecontrol\feature_restricted_zone_when_file_not_found
     Opens key:
                                                                     HKLM\software\microsoft\internet
 explorer\main\featurecontrol\feature_restricted_zone_when_file_not_found
                                                                     HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}
     Opens key:
                                                                     HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd\}
     Opens key:
     Opens key:
                                                                      HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
 fd2b31b3eefd}\treatas
                                                                      HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\ treatas
     Opens key:
     Opens key:
                                                                      HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
 fd2b31b3eefd}\inprocserver32
                                                                      HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\ \ in procserver 32
     Opens key:
                                                                      HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
     Opens key:
 fd2b31b3eefd}\inprocserverx86
                                                                     Opens key:
                                                                      HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
     Opens key:
 fd2b31b3eefd}\localserver32
                                                                      HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\localserver32
     Opens kev:
     Opens key:
                                                                      HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
 fd2b31b3eefd}\inprochandler32
                                                                     HKCR\clsid\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\ensuremath{\clsid}\
     Opens key:
     Opens key:
                                                                      HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
 fd2b31b3eefd}\inprochandlerx86
                                                                      HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprochandlerx86
     Opens key:
     Opens key:
                                                                      HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
 fd2b31b3eefd}\localserver
                                                                     HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\localserver
     Opens key:
     Opens key:
                                                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img
     Opens key:
                                                                     HKLM\software\microsoft\internet
 explorer\main\featurecontrol\feature_block_lmz_img
    Opens key:
                                                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\powrprof.dll
     Opens key:
                                                                      HKCU\control panel\powercfg
                                                                      HKLM\software\microsoft\windows\currentversion\controls folder\powercfg
     Opens kev:
     Opens key:
                                                                      HKCU\software\microsoft\internet
 explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
                                                                     HKLM\software\microsoft\internet
    Opens key:
 explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
     Opens key:
                                                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
```

HKLM\software\microsoft\internet

Opens key:

```
explorer\main\featurecontrol\feature_bufferbreaking_818408
  Opens key:
                                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:
                                  HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:
                                  HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
                                  \label{lem:hkcu} \verb+KCU\software\policies\microsoft\windows\currentversion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currenters
  Opens key:
settings\5.0\cache
  Opens key:
                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
  Opens key:
                                  HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
  Opens key:
                                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:
                                  HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:
                                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
  Opens key:
                                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
                                 HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_allow_long_international_filenames
  Opens key:
                                  HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
  Opens key:
                                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
                                 HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
  Opens key:
                                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
  Opens key:
                                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
  Opens key:
                                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                                 HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
  Opens key:
                                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                                 HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                                 HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature enable passport session store kb948608
  Opens key:
                                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
                                 HKLM\software\microsoft\internet
  Opens key:
explorer \verb|\main| featurecontrol| feature\_passport\_check\_302\_for\_success\_kb949059
  Opens key:
                                  HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
  Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000011
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
  Opens key:
Opens key:
```

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace_catalog 5 \setminus catalog_entries \setminus 0000000000001$

Opens key:

Opens key:

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615

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

filters\rpa

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

filters\rpa

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_include_port_in_spn_kb908209

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

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

options\rasman.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:

Opens key:

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

options\tapi32.dll

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

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

options\rasapi32.dll

Opens key: HKLM\software\microsoft\tracing\rasapi32

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

options\userenv.dll

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

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

folders

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist
Opens key: HKLM\system\currentcontrolset\control\session manager\environment
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

1757981266-507921405-1957994488-1003 Opens key: HKCU\environment

Opens key: HKCU\volatile environment

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

options\sensapi.dll

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

options\mswsock.dll

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

options\rasadhlp.dll

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

options\dnsapi.dll

Opens key: HKLM\system\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\rpc\securityservice

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

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

options\msv1_0.dll

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

options\rsaenh.dll

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

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

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

options\hnetcfg.dll

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

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

Opens key: HKCR\clsid\{00021401-0000-0000-0000000000046} Opens key: HKCU\software\classes\clsid\{00021401-0000-0000-c000-

000000000046}\treatas

Opens key: HKCR\clsid\{00021401-0000-0000-00000000000046}\treatas

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock

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

00000000046}\inprocserver32

Opens key: HKCR\clsid\{00021401-0000-0000-c000-00000000046}\inprocserver32

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

000000000046}\inprocserverx86

Opens key: HKCR\clsid\{00021401-0000-0000-c000-00000000046}\inprocserverx86

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

00000000046}\localserver32

Opens key: HKCR\clsid\{00021401-0000-0000-c000-0000000046}\localserver32

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

00000000046}\inprochandler32

Opens key: HKCR\clsid\{00021401-0000-0000-c000-00000000046}\inprochandler32

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

00000000046}\inprochandlerx86

Opens key: HKCR\clsid\{00021401-0000-0000-c000-00000000046}\inprochandlerx86
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\wshtcpip.dll

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

000000000046}\localserver

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

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

Opens key: HKCU\software\classes\.exe

Opens key: HKCR\.exe

Opens key: HKCU\software\classes\exefile

Opens key: HKCR\exefile

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

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

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

Opens key: HKCR\exefile\shellex\iconhandler

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

Opens key: HKCR\systemfileassociations\.exe

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

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

Opens key: HKCR\exefile\clsid

Opens key: HKCU\software\classes*\clsid

Opens key: HKCR*\clsid

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\ntshrui.dll

Opens key: HKLM\system\currentcontrolset\services\lanmanserver\defaultsecurity

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

5595fe6b30ee}\inprocserver32

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

Opens key: HKCU\software\soft-ware

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

options\msimg32.dll

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

Queries value:

 $HKLM \verb|\software| policies \verb|\microsoft| windows \verb|\software| for significant of the state of the software o$

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

nt\currentversion\compatibility32[700aa61e9dbd14abfcc633546a5be910]

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

compatibility[700aa61e9dbd14abfcc633546a5be910]

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

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

manager[criticalsectiontimeout]

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

Queries value: HKCR\interface[interfacehelperdisableall]

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

00000000046}[interfacehelperdisableall]

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

00000000046}[interfacehelperdisableallforole32]

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

HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
Queries value: HKLM\software\microsoft\windows\currentversion\internet

settings[disableimprovedzonecheck]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_protocol_lockdown[700aa61e9dbd14abfcc633546a5be910.exe]

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

Queries value: HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-

ab78-1084642581fb]

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

0000-00000000000001

```
HKLM\software\microsoft\ctf\systemshared[cuas]
 Oueries value:
                          HKCU\keyboard layout\toggle[language hotkey]
 Oueries value:
 Oueries value:
                          HKCU\keyboard layout\toggle[hotkey]
 Queries value:
                          HKCU\keyboard layout\toggle[layout hotkey]
 Oueries value:
                          HKLM\software\microsoft\ctf[enableanchorcontext]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
                          HKCU\software\microsoft\ctf[disable thread input manager]
 Oueries value:
 Oueries value:
                          HKLM\software\microsoft\rpc[maxrpcsize]
 Oueries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
                          HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[enabledhcp]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[leaseobtainedtime]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[leaseterminatestime]
 Oueries value:
c7d49d7cecdc}[dhcpserver]
 Queries value:
                          HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
 Queries value:
                          HKLM\system\wpa\pnp[seed]
                          HKLM\system\setup[osloaderpath]
 Oueries value:
 Queries value:
                          HKLM\system\setup[systempartition]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
 Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
 Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion[devicepath]
 Oueries value:
                          HKLM\software\microsoft\windows\currentversion\setup[loglevel]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\setup[logpath]
 Queries value:
                          HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
 Oueries value:
                          HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
 Queries value:
                          HKCR\http\shell\open\command[]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe[]
                          HKLM\software\microsoft\com3[com+enabled]
 Oueries value:
 Queries value:
                          HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
 Queries value:
                          HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]
                          HKLM\software\microsoft\com3[regdbversion]
 Oueries value:
                          HKCR\clsid\{8856f961-340a-11d0-a96b-
 Oueries value:
00c04fd705a2}\inprocserver32[inprocserver32]
                          HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32[]
 Oueries value:
 Queries value:
                          HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2\}[appid]
                          HKCR\clsid\{8856f961-340a-11d0-a96b-
 Oueries value:
00c04fd705a2}\inprocserver32[threadingmodel]
                          HKLM\software\microsoft\internet explorer\setup[iexplorelastmodifiedlow]
 Oueries value:
                          HKLM\software\microsoft\internet
 Oueries value:
explorer\setup[iexplorelastmodifiedhigh]
                          HKLM\system\currentcontrolset\control\session
 Queries value:
manager[safeprocesssearchmode]
                          HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib[]
 Queries value:
                          HKLM\software\microsoft\internet explorer\setup[installstarted]
 Oueries value:
 Queries value:
                          HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32[]
                          HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32[]
 Oueries value:
 Queries value:
                          HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32[]
 Queries value:
                          HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32[]
 Oueries value:
                          HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32[]
 Queries value:
                          HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
 Queries value:
                          HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
                          HKLM\software\policies\microsoft\internet
 Oueries value:
explorer\security[disablesecuritysettingscheck]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[flags]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[flags]
 Queries value:
                          \label{lem:hkcu} \verb+KKCU \software \verb+microsoft + windows + current version + internet
settings\zones\4[flags]
                          \label{lem:hkcu} \verb+KKCU \software \verb+microsoft + windows \verb+current version \verb+\internet+ \\
 Queries value:
settings[createuricachesize]
                          HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[createuricachesize]
 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[enablepunycode]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
```

```
settings[enablepunycode]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonethood]
 Queries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer[no properties my computer]
 Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
 Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
 Oueries value:
                          HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[]
 Oueries value:
11e3-9fc7-806d6172696f}[data]
 Queries value:
11e3-9fc7-806d6172696f}[generation]
                          HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
 Queries value:
409d6c4515e9}[drivemask]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
                          HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
 Oueries value:
 Oueries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer[forceactive desktop on]]
 Queries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer[noactive desktop]
HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]
 Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell]
 Queries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [separate process]
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
 Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\advanced[hidden]} \\
 Queries value:
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrybtn]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
                         HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
 Oueries value:
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
 Oueries value:
                          HKCR\directory[docobject]
                          HKCR\directory[browseinplace]
 Queries value:
                          HKCR\directory[isshortcut]
 Oueries value:
 Queries value:
                          HKCR\directory[alwaysshowext]
                          HKCR\directory[nevershowext]
 Queries value:
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.html[progid]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.html[application]
 Oueries value:
                          HKCR\.html[]
 Queries value:
                          HKCR\htmlfile\shellex\iconhandler[]
 Queries value:
                          HKCR\htmlfile[docobject]
 Oueries value:
                          HKCR\.html[perceivedtvpe]
 Queries value:
                          HKCR\systemfileassociations\text[docobject]
 Oueries value:
                          HKCR\htmlfile[browseinplace]
 Oueries value:
                          HKCR\systemfileassociations\text[browseinplace]
 Oueries value:
                          HKCR\htmlfile\clsid[]
 Queries value:
                          HKCR\htmlfile[isshortcut]
                          HKCR\systemfileassociations\text[isshortcut]
 Oueries value:
 Queries value:
                          HKCR\htmlfile[alwaysshowext]
```

```
Oueries value:
                          HKCR\systemfileassociations\text[alwaysshowext]
 Oueries value:
                          HKCR\htmlfile[nevershowext]
 Oueries value:
                          HKCR\systemfileassociations\text[nevershowext]
                          HKCU\software\microsoft\internet explorer\main[frametabwindow]
 Queries value:
 Oueries value:
                          HKLM\software\microsoft\internet explorer\main[frametabwindow]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[framemerging]
                          HKLM\software\microsoft\internet explorer\main[framemerging]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[sessionmerging]
 Oueries value:
 Oueries value:
                          HKLM\software\microsoft\internet explorer\main[sessionmerging]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[admintabprocs]
                          HKLM\software\microsoft\internet explorer\main[admintabprocs]
 Oueries value:
 Queries value:
                          HKLM\software\policies\microsoft\internet explorer\main[tabprocgrowth]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
 Oueries value:
                          HKLM\software\microsoft\internet explorer\main[tabprocgrowth]
 Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nofileurl]
                         HKLM\software\microsoft\internet explorer\main[navigationdelay]
 Oueries value:
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[urlencoding]
 Queries value:
                         HKCU\software\microsoft\internet explorer\international[acceptlanguage]
 Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nofilemenu]
                         HKLM\software\microsoft\windows\currentversion\policies\ratings[key]
 Oueries value:
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
                         HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[specialfolderscachesize]
                         HKCU\software\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\internet explorer[no3dborder]
 Queries value:
                         HKLM\software\microsoft\internet explorer[no3dborder]
 Queries value:
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[700aa61e9dbd14abfcc633546a5be910.exe]
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[*]
                         HKLM\software\microsoft\ole[maximumallowedallocationsize]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[proxyenable]
                         HKCR\.html[content type]
 Queries value:
                         HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_mime_sniffing[700aa61e9dbd14abfcc633546a5be910.exe]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing[*]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[istextplainhonored]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[700aa61e9dbd14abfcc633546a5be910.exe]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[*]
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-
 Oueries value:
00aa00686f13}\inprocserver32[inprocserver32]
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[]
 Queries value:
                         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
 Oueries value:
explorer\main\featurecontrol\feature_legacy_dispparams[700aa61e9dbd14abfcc633546a5be910.exe]
                         HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_legacy_dispparams[*]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching[700aa61e9dbd14abfcc633546a5be910.exe]
 Oueries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching[*]
                         HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
                         HKLM\software\microsoft\internet explorer\application
 Queries value:
compatibility[700aa61e9dbd14abfcc633546a5be910.exe]
 Queries value:
                         HKCU\software\microsoft\internet explorer\domstorage[totallimit]
 Oueries value:
                         HKCU\software\microsoft\internet explorer\domstorage[domainlimit]
 Queries value:
                         HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinset]
                         HKCU\software\microsoft\windows
 Oueries value:
nt\currentversion\windows[dragscrolldelay]
 Queries value:
                         HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinterval]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[700aa61e9dbd14abfcc633546a5be910.exe]
                         HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_restrict_filedownload[*]
 Queries value:
                         HKCR\protocols\handler\about[clsid]
                         HKCR\clsid\{3050f406-98b5-11cf-bb82-
 Oueries value:
```

00aa00bdce0b}\inprocserver32[inprocserver32]

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

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

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

00aa00bdce0b}\inprocserver32[threadingmodel]

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

Oueries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_legacy_dlcontrol_behaviors[700aa61e9dbd14abfcc633546a5be910.exe]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_legacy_dlcontrol_behaviors[*]

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

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

explorer\main[use_dlgbox_colors]

Queries value: HKCU\software\microsoft\internet explorer\main[use_dlgbox_colors] $\label{lem:hklm} \verb+Kklm \+ software \+ policies \+ microsoft \+ internet explorer \+ main[anchor]$ Queries value:

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

videos1

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

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

explorer\main[play_background_sounds]

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

Oueries value: HKCU\software\microsoft\internet explorer\main[play_animations]

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

explorer\main[print_background]

HKCU\software\microsoft\internet explorer\main[print_background] Queries value: HKCU\software\microsoft\internet explorer\main[use stylesheets] Oueries value: Queries value: HKLM\software\policies\microsoft\internet explorer\main[smoothscroll] Oueries value: HKCU\software\microsoft\internet explorer\main[smoothscroll] Queries value: HKLM\software\policies\microsoft\internet explorer\main[xmlhttp] Oueries value: HKCU\software\microsoft\internet explorer\main[xmlhttp] Queries value:

HKLM\software\policies\microsoft\internet explorer\main[show image

placeholders]

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

debugger]

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

composition]

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

autoimageresize]

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

Queries value: HKCU\software\microsoft\internet explorer\main[usethemes] Queries value: HKCU\software\microsoft\internet explorer\main[usehr] $HKCU \setminus software \setminus microsoft \setminus internet \ explorer \setminus main[q300829]$ Oueries value: Queries value: HKCU\software\microsoft\internet explorer\main[cleanup htcs]

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

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

Queries value: HKCU\software\microsoft\internet explorer\main[domstorage] HKLM\software\microsoft\internet explorer\main[domstorage] Oueries value:

Oueries value: HKCU\software\microsoft\internet

explorer\international[default_codepage]

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

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

HKCU\software\microsoft\internet explorer\settings[anchor color] Oueries value: Oueries value: HKCU\software\microsoft\internet explorer\settings[anchor color visited] Oueries value: HKCU\software\microsoft\internet explorer\settings[anchor color hover] Queries value: HKCU\software\microsoft\internet explorer\settings[always use my colors] $\label{lem:hkcu} \mbox{HKCU\software\mbox{$\mbox{microsoft\internet explorer\settings[always use my font]}} \label{lem:hkcu}$ Oueries value:

sizel

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

settings[disablecachingofsslpages]

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[700aa61e9dbd14abfcc633546a5be910.exe]

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

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

settings\zones\0[2700]

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

settings\zones\0[2700]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_xssfilter[700aa61e9dbd14abfcc633546a5be910.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\0[2106]

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

settings\zones\0[2106]

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

settings\zones\0[1400]

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

settings[warnonintranet]

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

settings[warnonintranet]

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

settings\zonemap[autodetect]

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

f4ceaaf59cfc}\inprocserver32[inprocserver32]

 $Queries\ value: \\ HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\ \ value: \\ HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\ \ \ value: \\ HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\ \ \ \ \ value: \\ Value$

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

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

f4ceaaf59cfc}\inprocserver32[threadingmodel]

 $\label{lem:lem:queries} Queries value: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}\[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:hklm} HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\tem\{5130a009-5540-4fcf-97eb-aad33fc0ee09}\[description] \\ Queries value: <math display="block"> \label{lem:hklm} HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\tem\{7ae86bb7-262c-431e-9111-c974b6b7cac3}\[description] \\ Queries value: <math display="block"> \label{lem:hklm} HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\tem\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}\[description]$

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

folders[recent]

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]

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

settings\zones\0[1201]

Queries value: HKLM\system\currentcontrol\st\control\nls\locale[00000409] Queries value: HKLM\system\currentcontrol\set\control\nls\language groups[1]

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

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

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

settings\zones\0[2000]

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

history[daystokeep]

Queries value: HKCU\software\microsoft\ftp[use web based ftp]

Queries value: HKCU\software\microsoft\internet

explorer\services[selectionactivitybuttondisable]

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

manager\appcompatibility[disableappcompat]

Queries value: HKLM\system\wpa\mediacenter[installed]

Queries value:

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

Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]

Queries value:

 $HKLM software \verb|\policies| microsoft \verb|\windows| safer \verb|\codeidentifiers| 0 \verb|\paths| { dda3f824-d8cb-441b-834d-be2efd2c1a33} [itemdata]$

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}[saferflags]

Queries value:

Queries value:

Oueries value:

Queries value:

Oueries value:

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

settings[cointernetcombineiuricachesize]

Queries value:

Queries value:

Queries value:

Queries value:

 $\label{thm:local-bound} HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f\}[itemdata]}$

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{81d1fe15-dd9d-4762-b16d-7c29ddecae3f\} [hashalg]$

Queries value:

 $\label{thm:mass} HKLM software \verb|policies| microsoft| windows \verb|safer| code identifiers| 0 hashes | \{81d1fe15-dd9d-4762-b16d-7c29ddecae3f\} | [itemsize] | the safety code identifiers |$

Queries value:

Queries value:

 $\label{thm:microsoft} $$HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}\ [itemdata]$

Queries value: HKLM\software\microsoft\internet

 $\verb|explorenmainfeaturecontrol| feature_subdownload_lockdown[700aa61e9dbd14abfcc633546a5be910.exe]|$

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

. Queries value

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{94e3e076-8f53-42a5-8411-085bcc18a68d\} \ [hashalg]$

Queries value:

 $\label{thm:local-basis} HKLM \software \policies \microsoft \windows \safer \code identifiers \one \noise \noise$

Queries value:

 $\label{thm:local-bound} $HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}\ [saferflags]$

Queries value:

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

Oueries value: HKCR\.css[content type]

Oueries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe$

b91490411bfc}[hashalg]

Oueries value:

b91490411bfc}[itemsize]

Oueries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe$ b91490411bfc}[saferflags]

 $\label{lem:hklm} \verb+Kklm/software/microsoft/internet explorer/default behaviors[discovery]$ Oueries value:

Queries value:

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

Oueries value:

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

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

folders[cache] Queries value:

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

HKCR\clsid\{3050f4cf-98b5-11cf-bb82-Oueries value:

00aa00bdce0b}\inprocserver32[inprocserver32]

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

 $\label{local-bbs2-00aa00bdce0b} HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\ [appid]$ Oueries value:

HKCR\clsid\{3050f4cf-98b5-11cf-bb82-Queries value:

00aa00bdce0b}\inprocserver32[threadingmodel] Queries value: HKCR\.png[content type]

HKCR\clsid\{30c3b080-30fb-11d0-b724-Queries value:

00aa006c1a01}\inprocserver32[inprocserver32]

HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[] Oueries value:

HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}[appid] Queries value:

HKCR\clsid\{30c3b080-30fb-11d0-b724-Oueries value:

00aa006c1a01}\inprocserver32[threadingmodel]

HKCR\clsid\{6a01fda0-30df-11d0-b724-Queries value:

00aa006c1a01}\inprocserver32[inprocserver32]

HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32[] Oueries value:

HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}[appid] Queries value:

HKCR\clsid\{6a01fda0-30df-11d0-b724-Oueries value:

00aa006c1a01}\inprocserver32[threadingmodel]

HKCR\mime\database\content type\image/bmp\bits[0] Queries value: Queries value: HKCR\mime\database\content type\image/gif\bits[0] Oueries value: HKCR\mime\database\content type\image/jpeg\bits[0] HKCR\mime\database\content type\image/pjpeg\bits[0] Queries value: Oueries value: HKCR\mime\database\content type\image/png\bits[0] Queries value: HKCR\mime\database\content type\image/x-png\bits[0] HKCR\mime\database\content type\image/x-wmf\bits[0] Oueries value:

HKCR\mime\database\content type\image/x-png[image filter clsid] Queries value:

Queries value: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-

00a0c913f750}\inprocserver32[inprocserver32]

HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[] Oueries value:

Queries value: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}[appid]

HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-Oueries value:

00a0c913f750}\inprocserver32[threadingmodel] Queries value: HKCR\.gif[content type]

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

settings[syncmode5]

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

settings\5.0\cache[sessionstarttimedefaultdeltasecs]

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

settings\5.0\cache[signature]

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

Queries value:

settings\5.0\cache\content[peruseritem]

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

settings\5.0\cache\content[cacheprefix] Oueries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\content[cachelimit]

Queries value: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}$

settings\5.0\cache\cookies[peruseritem]

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

settings\5.0\cache\cookies[peruseritem]

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

settings\5.0\cache\cookies[cacheprefix] Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\cookies[cachelimit]

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

settings\5.0\cache\history[peruseritem] Oueries value: HKLM\software\microsoft\windows\currentversion\internet

settings\5.0\cache\history[peruseritem]

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

folders[history]

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

settings\5.0\cache\history[cacheprefix]

```
Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cachepath]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheprefix]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cacheoptions]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\ietld[cacherepair]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\ietld[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\ietld[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\ietld[cacheoptions]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
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]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cacherepair]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
                         HKCR\clsid\{e569bde7-a8dc-47f3-893f-
 Oueries value:
fd2b31b3eefd}\inprocserver32[inprocserver32]
 Queries value:
                          HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\nprocserver32[]
 Oueries value:
                          HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd\}[appid]
 Queries value:
                          HKCR\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32[threadingmodel]
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Oueries value:
folders[local appdata]
 Queries value:
                          HKCU\control panel\powercfg[adminmaxsleep]
                          HKCU\control panel\powercfg[adminmaxvideotimeout]
 Oueries value:
 Queries value:
                          {\it HKLM} \ software \verb|\microsoft| windows \verb|\currentversion| controls
```

```
folder\powercfg[lastid]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[fromcachetimeout]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
 Queries value:
                             HKLM\software\policies\microsoft\internet
explorer\main[security_hklm_only]
                             \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
 Oueries value:
settings[certificaterevocation]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
 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[disablepassport]
 Oueries value:
                             HKCU\software\microsoft\windows\currentversion\internet
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
 Queries value:
settings[proxyhttp1.1]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[enablenegotiate]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablebasicoverclearchannel]
                            HKCU\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
                            HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[clientauthbuiltinui]
                            \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[disableworkerthreadhibernation]
                             HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablereadrange]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketreceivebufferlength]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[keepalivetimeout]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsper1_0server]
 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[maxconnectionsperproxy]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connecttimeout]
                             HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connecttimeout]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
                             HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connectretries]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendtimeout]
 Queries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[receivetimeout]
                             HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[receivetimeout]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[scavengecachelowerbound]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelimit]
```

```
Oueries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[ftpdefaultexpirytimesecs]
                          HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[700aa61e9dbd14abfcc633546a5be910.exe]
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[leashlegacycookies]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablent4rascheck]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dialupuselansettings]
                          HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dialupuselansettings]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendextracrlf]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypassftptimecheck]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[releasesocketduringauth]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[releasesocketduring401auth]
 Oueries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[wpadsearchalldomains]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasshttpnocachecheck]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
                          HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasssslnocachecheck]
 Oueries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
 Oueries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                          HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sharecredswithwinhttp]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dnscacheenabled]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonpost]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecross
                         ing]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonbadcertsending]
 Queries value:
                          \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[warnonbadcertrecving]
 Queries value:
                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[warnonpostredirect]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
```

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

Queries value: HKCU\softw settings[warnonhttpstohttpredirect] Queries value:

settings[alwaysdrainonredirect]

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

Queries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]

 Oueries 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000004[packedcatalogitem]

 Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries \ 0000000000005 \ [packed catalog item] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
 Queries value:
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
- Queries value:

 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000009[packedcatalogitem]
- Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
 Oueries value:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 0000000000001 \ [providerid] \ Oueries \ value:$
- 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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
- 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\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[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\000000000002[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Queries 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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
 Oueries value:
- $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws 2_32 numhandle buckets]$

```
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2 32spincount1
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[enableautodial]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[urlencoding]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[truncatefilename]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[badproxyexpirestime]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
 Oueries 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]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
 Oueries value:
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
 Oueries value:
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
 Queries 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]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
 Queries value:
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
 Oueries value:
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
 Queries value:
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
 Queries value:
 Oueries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
 Queries value:
 Oueries value:
                          \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ drivers 32 [mixer 2]
 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]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32maxnumrequestretries]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32requestretrytimeout]
 Oueries value:
                          HKLM\software\microsoft\tracing[enableconsoletracing]
                          HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
 Queries value:
 Queries value:
                          HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
 Oueries value:
                          HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
                          HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
 Queries value:
 Queries value:
                          HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
 Queries value:
                          HKLM\software\microsoft\tracing\rasapi32[filedirectory]
                          \label{thm:local_hammon} \mbox{\tt HKLM} \mbox{\tt software} \mbox{\tt microsoft} \mbox{\tt windows} \mbox{\tt current} \mbox{\tt version} \mbox{\tt explorer} \mbox{\tt user} \mbox{\tt shell}
 Oueries value:
folders[common appdata]
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
                          HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\winlogon[chkaccdebuglevel]
                          HKLM\system\currentcontrolset\control\productoptions[producttype]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Oueries value:
folders[personal]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local settings]
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\winlogon[rsopdebuglevel]
                          HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
 Oueries value:
 Oueries value:
                          HKLM\software\microsoft\windows
nt\currentversion\profilelist[profilesdirectory]
```

Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[allusersprofile]

Oueries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[defaultuserprofile] Oueries value: HKLM\software\microsoft\windows\currentversion[programfilesdir] Queries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir] HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-Oueries value: 1757981266-507921405-1957994488-1003[profileimagepath] Queries value: HKCU\software\microsoft\windows $\verb|nt\currentversion\winlogon[parseautoexec]| \\$ Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[appdata] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[migrateproxy] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[proxyserver] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[proxyoverride] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[autoconfigurl] $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Queries value: settings\connections[savedlegacysettings] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\connections[defaultconnectionsettings] HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll] Oueries value: Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]

HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]

 $HKLM \verb| system| current control set \verb| services| dns cache \verb| parameters[used omain name devolution]|$

HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]

 $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [prioritize record data]$

HKLM\svstem\currentcontrolset\services\dnscache\parameters[allowungualifiedguerv]

HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]

HKLM\svstem\currentcontrolset\services\dnscache\parameters[screenbadtlds] Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers] Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [filter clusterip]$

Queries value:

HKLM\svstem\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]

Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]

Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Queries value:

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]

HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]

Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]

Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]

Queries value:

Oueries value:

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl] 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] Queries 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] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts] Queries value: c7d49d7cecdc}[queryadaptername] c7d49d7cecdc}[disableadapterdomainname] c7d49d7cecdc}[registrationenabled] Queries value: c7d49d7cecdc}[registeradaptername] c7d49d7cecdc}[registrationmaxaddresscount] c7d49d7cecdc}[maxnumberofaddressestoregister] $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4300-abe3-4300-a$ c7d49d7cecdc}[domain] Oueries value: c7d49d7cecdc}[dhcpdomain] Queries value: c7d49d7cecdc}[ipautoconfigurationenabled] Oueries value: c7d49d7cecdc}[addresstype] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[nameserver] Queries value: c7d49d7cecdc}[dhcpnameserver] HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [dnsnbtlookuporder]$ Queries value: $HKLM \ software \ microsoft \ strong$ cryptographic provider[type] Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[image path] Oueries value: HKLM\software\microsoft\rpc\securityservice[10] Queries value: HKLM\system\currentcontrolset\control\securityproviders[securityproviders] HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name] Oueries value: Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment] Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]

 $HKLM \setminus system \setminus current control \setminus lsa \setminus spicache \setminus msaps spc.dll[version]$

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

Queries value:

Oueries value:

Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type] Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize] HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment] Oueries value: Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities] HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version] Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type] Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name] HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities] HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid] Oueries value: Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version] Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type] Oueries value: HKLM\system\currentcontrol\set\control\lsa\sspicache\msnsspc.dll[tokensize] Queries value: HKLM\software\microsoft\cryptography[machineguid] HKCU\software\microsoft\windows\currentversion\explorer\user shell Queries value: folders[desktop] Queries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel] Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [mapping]$ Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength] Queries value: Queries value: HKCR\clsid\{00021401-0000-0000-c000-00000000046}\inprocserver32[inprocserver32] HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname] HKCR\clsid\{00021401-0000-0000-c000-0000000046}\inprocserver32[] Queries value: HKCR\clsid\{00021401-0000-0000-c000-00000000046}[appid] Queries value: HKCR\clsid\{00021401-0000-0000-c000-Queries value: 00000000046}\inprocserver32[threadingmodel] HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[comparejunctionness] HKLM\software\microsoft\windows\currentversion\explorer\user shell Queries value: folders[common documents] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[common desktop] Queries value: HKCR\.exe[] HKCR\exefile[docobject] Oueries value: HKCR\exefile[browseinplace] Oueries value: Queries value: HKCR\exefile[isshortcut] Queries value: HKCR\exefile[alwaysshowext] Oueries value: HKCR\exefile[nevershowext] Queries value: HKCR\network\sharinghandler[] Oueries value: HKLM\system\currentcontrolset\services\lanmanserver\defaultsecurity[srvsvcdefaultshareinfo] HKCU\software\microsoft\windows\currentversion\explorer\user shell Oueries value: folders[start menu] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[common start menu] HKCU\software\microsoft\windows\currentversion\explorer\user shell Queries value: folders[my pictures] Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir (x86)] HKLM\software\microsoft\windows\currentversion\explorer\user shell Oueries value: folders[commonpictures] HKCR\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\inprocserver32[] Queries value: Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[noshareddocuments] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[commonmusic] Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[commonvideo] Queries value: HKLM\software\microsoft\internet explorer\main[maxrenderline]

HKLM\software\microsoft\cryptography\rng[seed] Value changes:

Value changes: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}$ settings\zonemap[proxybypass]

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

settings\zonemap[intranetname]

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

settings\zonemap[uncasintranet]

Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[autodetect]

Value changes:

 $HKCU \ software \ microsoft \ windows \ current version \ lex plorer \ mountpoints \ 2 \ \{f90255c2-6bc4-11e3-9fc7-6bc4-11e3-$

806d6172696f}[baseclass]

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

folders[cookies]

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

folders[history]

 $\label{thm:condition} Value\ changes: \\ HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus shell \\$

folders[local appdata]

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

folders[common appdata]

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

folders[appdata]

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

settings[proxyenable]

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

settings\connections[savedlegacysettings]

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

folders[desktop]

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

folders[personal]

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

folders[common documents]

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

folders[common desktop]

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

folders[start menu]

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

folders[common start menu]

Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[my

pictures]

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

folders[commonpictures]

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

folders[commonmusic]

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

folders[commonvideo]