Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

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 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]
3 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\ZonesLockedCacheCounterMutex
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\1VtP0S1F1O2ZtG0W1T1C1PtP1V
Creates semaphore:	\BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}
Creates semaphore:	\BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}

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\Temp\ish10855279\css\ie6_main.css

```
  Creates:                 C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\css\main.css
  Creates:                 C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
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
  Creates:                 C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\images
  Creates:                 C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\images\button-bg.png
  Creates:                 C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\images\progress-bg-corner.png
  Creates:                 C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\images\progress-bg.png
  Creates:                 C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\images\progress-bg2.png
  Creates:                 C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\progress-bar.css
  Creates:                 C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\csshover3.htc
  Creates:                 C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\form.bmp.Mask
  Creates:                 C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\images
  Creates:                 C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\BG.png
  Creates:                 C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Close.png
  Creates:                 C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Close_Hover.png
  Creates:                 C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Color_Button.png
  Creates:                 C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Color_Button_Hover.png
  Creates:                 C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Grey_Button.png
  Creates:                 C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Grey_Button_Hover.png
  Creates:                 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
  Creates:                 C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Pause_Button.png
  Creates:                 C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Progress.png
  Creates:                 C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\ProgressBar.png
  Creates:                 C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Quick_Specs.png
  Creates:                 C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Resume_Button.png
  Creates:                 C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\locale
  Creates:                 C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\locale\DE.locale
  Creates:                 C:\Documents and Settings\Admin\Local
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
  Creates:                 C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\bootstrap_3733.html
  Creates:                 C:\Documents and Settings\Admin\Local Settings\Temp\00A69D39.log
  Creates:                 C:\Documents and Settings\Admin\Local
Settings\Temp\ICReinstall_700aa61e9dbd14abfcc633546a5be910.exe
  Creates:                 C:\Documents and Settings\Admin\Desktop\Continue CCleaner
Installation.lnk
  Creates:                 C:\Documents and Settings\Admin\Local Settings\Temp\00A6A078.log
  Creates:                 C:\Documents and Settings\Admin\Local Settings\Temp\is956058749
  Creates:                 C:\Documents and Settings\Admin\Local
Settings\Temp\is956058749\10920075_Setup.EXE
  Opens:                   C:\WINDOWS\Prefetch\700AA61E9DBD14ABFCC633546A5BE-0CD25A82.pf
  Opens:                   C:\Documents and Settings\Admin
  Opens:                   C:\WINDOWS\system32\imm32.dll
  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
  Opens:                   C:\WINDOWS\system32\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-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
  Opens:                  C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
  Opens:                  C:\WINDOWS\WindowsShell.Manifest
  Opens:                  C:\WINDOWS\WindowsShell.Config
  Opens:                  C:\WINDOWS\system32\URLMON.DLL.123.Manifest
  Opens:                  C:\WINDOWS\system32\URLMON.DLL.123.Config
  Opens:                  C:\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
  Opens:                  C:\WINDOWS\system32\MSCTF.dll
  Opens:                  C:\WINDOWS\system32\MSCTFIME.IME
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\00A5A36F.log
  Opens:                  C:\WINDOWS\Temp\2b018457-30d9-4422-b29c-98224f056ad2
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\css\ie6_main.css
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\css\main.css
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\browse.css
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\button.css
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\checkbox.css
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\images
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\images\button-bg.png
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\images\progress-bg-corner.png
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\images\progress-bg.png
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\images\progress-bg2.png
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\progress-bar.css
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\csshover3.htc
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\form.bmp.Mask
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\images
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\BG.png
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Close.png
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Close_Hover.png
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Color_Button.png
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Color_Button_Hover.png
  Opens:                  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
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Icon_Generic.png
  Opens:                  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
  Opens:                  C:\Documents and Settings\Admin\Local
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
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Resume_Button.png
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\locale
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\locale\DE.locale
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\locale\EN.locale
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\sdk
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\sdk\exceptlist.txt
  Opens:                  C:\WINDOWS\system32\iphlpapi.dll
  Opens:                  C:\WINDOWS\system32\ws2_32.dll
  Opens:                  C:\WINDOWS\system32\ws2help.dll
  Opens:                  C:\WINDOWS\system32\mprapi.dll
  Opens:                  C:\WINDOWS\system32\activeds.dll
  Opens:                  C:\WINDOWS\system32\adsldpc.dll
  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:                  C:\
  Opens:                  C:\Program Files\Internet Explorer
  Opens:                  C:\Program Files\Internet Explorer\iexplore.exe
  Opens:                  C:\WINDOWS\system32\clbcatq.dll
  Opens:                  C:\WINDOWS\system32\comres.dll
  Opens:                  C:\WINDOWS\Registration\R000000000007.clb
  Opens:                  C:\WINDOWS\system32\ieframe.dll
  Opens:                  C:\WINDOWS\system32\ieframe.dll.123.Manifest
  Opens:                  C:\WINDOWS\system32\ieframe.dll.123.Config
  Opens:                  C:\WINDOWS\system32\en-US\ieframe.dll.mui
  Opens:                  C:\WINDOWS\system32\sxs.dll
  Opens:                  C:\WINDOWS\system32\MSIMTF.dll
  Opens:                  C:\Documents and Settings
  Opens:                  C:\Documents and Settings\Admin\Local Settings
  Opens:                  C:\WINDOWS\system32\mlang.dll
  Opens:                  C:\WINDOWS\system32\MLANG.dll.123.Manifest
  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:                  C:\WINDOWS\AppPatch\sysmain.sdb
  Opens:                  C:\WINDOWS\AppPatch\systest.sdb
  Opens:                  C:\WINDOWS\Temp
  Opens:                  C:\WINDOWS
  Opens:                  C:\DOCUME~1\Admin\LOCALS~1\Temp\ish10855279\script\
  Opens:                  C:\windows\temp\700aa61e9dbd14abfcc633546a5be910.exe.Manifest
  Opens:                  C:\windows\temp\700aa61e9dbd14abfcc633546a5be910.exe.Config
  Opens:                  C:\WINDOWS\system32\iepeers.dll
  Opens:                  C:\WINDOWS\system32\winspool.drv
  Opens:                  C:\WINDOWS\system32\iepeers.dll.123.Manifest
  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
  Opens:                  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
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
  Opens:                  C:\WINDOWS\Fonts\arialbd.ttf
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT
  Opens:                  C:\WINDOWS\system32\powrprof.dll
  Opens:                  C:\WINDOWS\system32\rasapi32.dll
  Opens:                  C:\WINDOWS\system32\rasman.dll
  Opens:                  C:\WINDOWS\system32\tapi32.dll
  Opens:                  C:\WINDOWS\system32\winmm.dll
  Opens:                  C:\WINDOWS\system32\TAPI32.dll.124.Manifest
  Opens:                  C:\WINDOWS\system32\TAPI32.dll.124.Config
  Opens:                  C:\AUTOEXEC.BAT
  Opens:                  C:\Documents and Settings\All Users\Application
Data\Microsoft\Network\Connections\Pbk
  Opens:                  C:\WINDOWS\system32\ras
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\Network\Connections\Pbk\
  Opens:                  C:\WINDOWS\system32\sensapi.dll
  Opens:                  C:\WINDOWS\system32\mswsock.dll
  Opens:                  C:\WINDOWS\system32\rasadhlp.dll
  Opens:                    C:\WINDOWS\system32\dnsapi.dll
  Opens:                    C:\Documents and Settings\Admin\Local Settings\Temp\00A69D39.log
  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
  Opens:                    C:\WINDOWS\system32\crypt32.dll
  Opens:                    C:\WINDOWS\system32\hnetcfg.dll
  Opens:                    C:\WINDOWS\system32\wshtcpip.dll
  Opens:                    C:\Documents and Settings\Admin\My Documents\desktop.ini
  Opens:                    C:\Documents and Settings\All Users
  Opens:                    C:\Documents and Settings\All Users\Documents\desktop.ini
  Opens:                    C:\WINDOWS\system32\linkinfo.dll
  Opens:                    C:\WINDOWS\system32\ntshrui.dll
  Opens:                    C:\WINDOWS\system32\ntshrui.dll.123.Manifest
  Opens:                    C:\WINDOWS\system32\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
  Opens:                    C:\Documents and Settings\All Users\Documents\My Pictures\Desktop.ini
  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
  Opens:                    C:\Documents and Settings\Admin\Local
Settings\Temp\is956058749\10920075_Setup.EXE
  Opens:                    C:\WINDOWS\system32\en-US\jscript.dll.mui
  Writes to:                C:\Documents and Settings\Admin\Local Settings\Temp\00A5A36F.log
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\css\ie6_main.css
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\css\main.css
  Writes to:                C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\browse.css
  Writes to:                C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\button.css
  Writes to:                C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\checkbox.css
  Writes to:                C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\images\button-bg.png
  Writes to:                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
  Writes to:                C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\images\progress-bg2.png
  Writes to:                C:\Documents and Settings\Admin\Local Settings\Temp\ish10855279\css\sdk-
ui\progress-bar.css
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\csshover3.htc
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\form.bmp.Mask
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\BG.png
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Close.png
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Close_Hover.png
  Writes to:                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
  Writes to:                C:\Documents and Settings\Admin\Local
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
  Writes to:                C:\Documents and Settings\Admin\Local
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
  Writes to:                C:\Documents and Settings\Admin\Local
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
  Writes to:                 C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\locale\DE.locale
  Writes to:                 C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\locale\EN.locale
  Writes to:                 C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\sdk\exceptlist.txt
  Writes to:                 C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\bootstrap_3733.html
  Writes to:                 C:\Documents and Settings\Admin\Local Settings\Temp\00A69D39.log
  Writes to:                 C:\Documents and Settings\Admin\Local
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\R000000000007.clb
  Reads from:                C:\WINDOWS\system32\ieframe.dll
  Reads from:                C:\Documents and Settings\Admin\Local
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
  Reads from:                C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\BG.png
  Reads from:                C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Quick_Specs.png
  Reads from:                C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\locale\EN.locale
  Reads from:                C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Grey_Button.png
  Reads from:                C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Color_Button.png
  Reads from:                C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Close.png
  Reads from:                C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Loader.gif
  Reads from:                C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\ProgressBar.png
  Reads from:                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
  Reads from:                C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Resume_Button.png
  Reads from:                C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\form.bmp.Mask
  Reads from:                C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Close_Hover.png
  Reads from:                C:\Documents and Settings\Admin\Local
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
  Reads from:                C:\Documents and Settings\Admin\Local
Settings\Temp\ICReinstall_700aa61e9dbd14abfcc633546a5be910.exe
  Reads from:                C:\Documents and Settings\Admin\My Documents\desktop.ini
  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
  Reads from:                C:\Documents and Settings\Admin\Application Data\desktop.ini
  Reads from:                C:\Documents and Settings\Admin\My Documents\My Pictures\Desktop.ini
  Reads from:                C:\Documents and Settings\All Users\Documents\My Pictures\Desktop.ini
  Reads from:                C:\Documents and Settings\All Users\Documents\My Music\Desktop.ini
  Reads from:                C:\Documents and Settings\All Users\Documents\My Videos\Desktop.ini
  Reads from:                C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\images\Icon_Generic.png
  Reads from:                C:\Documents and Settings\Admin\Local Settings\Temp\00A6A078.log
  Deletes:                   C:\Documents and Settings\Admin\Local Settings\Temp\00A5A36F.log
  Deletes:                   C:\Documents and Settings\Admin\Local
Settings\Temp\ish10855279\bootstrap_3733.html
  Deletes:                   C:\Documents and Settings\Admin\Local Settings\Temp\00A69D39.log
  Deletes:                   C:\Documents and Settings\Admin\Local Settings\Temp\00A6A078.log
```

Network Events

DNS query:	`os.softwarenetcdn.com`
DNS query:	`www.soft-ware.net`
DNS response:	`os.softwarenetcdn.com ⇒ 54.77.202.184`
DNS response:	`os.softwarenetcdn.com ⇒ 52.31.134.147`
DNS response:	`os.softwarenetcdn.com ⇒ 54.194.194.239`
DNS response:	`www.soft-ware.net ⇒ 104.27.164.7`
DNS response:	`www.soft-ware.net ⇒ 104.27.165.7`
Connects to:	`54.77.202.184:80`
Connects to:	`104.27.164.7:80`
Sends data to:	`8.8.8.8:53`
Sends data to:	`os.softwarenetcdn.com:80 (54.77.202.184)`
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

Creates key:	`HKCU\software\microsoft\windows\currentversion\internet settings`
Creates key:	`HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-806d6172696f}\`
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`
Creates key:	`HKLM\software\microsoft\windows\currentversion\explorer\user shell folders`
Creates key:	`HKCU\software\microsoft\windows nt\currentversion\winlogon`
Creates key:	`HKLM\software\microsoft\windows\currentversion\explorer\shell folders`
Creates key:	`HKCU\software\microsoft\windows\currentversion\internet settings\connections`
Creates key:	`HKCU\software\microsoft\windows nt\currentversion\network\location awareness`
Creates key:	`HKLM\system\currentcontrolset\services\tcpip\parameters`
Deletes value:	`HKCU\software\microsoft\windows\currentversion\internet settings[proxyserver]`
Deletes value:	`HKCU\software\microsoft\windows\currentversion\internet settings[proxyoverride]`
Deletes value:	`HKCU\software\microsoft\windows\currentversion\internet settings[autoconfigurl]`
Opens key:	`HKLM\software\microsoft\windows nt\currentversion\image file execution options\700aa61e9dbd14abfcc633546a5be910.exe`
Opens key:	`HKLM\system\currentcontrolset\control\terminal server`
Opens key:	`HKLM\software\microsoft\windows nt\currentversion\image 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`
Opens key:	`HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll`
Opens key:	`HKLM\software\microsoft\windows nt\currentversion\image file execution options\secur32.dll`
Opens key:	`HKLM\software\microsoft\windows nt\currentversion\image file execution options\rpcrt4.dll`
Opens key:	`HKLM\software\microsoft\windows nt\currentversion\image file execution options\advapi32.dll`
Opens key:	`HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll`
Opens key:	`HKLM\software\microsoft\windows nt\currentversion\image file execution options\ole32.dll`
Opens key:	`HKLM\software\microsoft\windows nt\currentversion\image file execution options\oleaut32.dll`
Opens key:	`HKLM\software\microsoft\windows nt\currentversion\image file execution options\comctl32.dll`
Opens key:	`HKLM\system\currentcontrolset\control\error message instrument\`
Opens key:	`HKLM\system\currentcontrolset\control\error message instrument`
Opens key:	`HKLM\software\microsoft\windows nt\currentversion\gre_initialize`
Opens key:	`HKLM\software\microsoft\windows nt\currentversion\compatibility32`
Opens key:	`HKLM\software\microsoft\windows nt\currentversion\ime compatibility`
Opens key:	`HKLM\software\microsoft\windows nt\currentversion\windows`
Opens key:	`HKLM\software\microsoft\windows nt\currentversion\winlogon`
Opens key:	`HKLM\`
Opens key:	`HKLM\software\microsoft\windows nt\currentversion\diagnostics`

```
  Opens key:                HKLM\software\microsoft\ole
  Opens key:                HKCR\interface
  Opens key:                HKCR\interface\{00020400-0000-0000-c000-000000000046}
  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\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:                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:                HKLM\software\microsoft\windows nt\currentversion\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
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\700aa61e9dbd14abfcc633546a5be910.exe\rpcthreadpoolthrottle
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                HKLM\system\currentcontrolset\control\computername
  Opens key:                HKLM\system\currentcontrolset\control\computername\activecomputername
  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\
  Opens key:                HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
  Opens key:                HKLM\system\currentcontrolset\services\netbt\parameters
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
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
  Opens key:                HKLM\system\currentcontrolset\services\ldap
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\adsldpc.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\atl.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\activeds.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rtutils.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\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
  Opens key:                HKLM\software\microsoft\windows\currentversion\setup
  Opens key:                HKLM\software\microsoft\windows\currentversion
  Opens key:                HKLM\software\microsoft\windows\currentversion\setup\apploglevels
  Opens key:                HKLM\system\currentcontrolset\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
  Opens key:                HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe
  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
  Opens key:                HKLM\software\microsoft\com3\debug
  Opens key:                HKLM\software\classes
  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
  Opens key:                HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas
  Opens key:                HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32
  Opens key:                HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\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
  Opens key:                HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandler32
  Opens key:                HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandlerx86
  Opens key:                HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\localserver
```

```
  Opens key:                 HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\localserver
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ieframe.dll
  Opens key:                 HKLM\software\microsoft\internet explorer\setup
  Opens key:                 HKCU\software\classes\interface\{eab22ac1-30c1-11cf-a7eb-
0000c05bae0b}\typelib
  Opens key:                 HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib
  Opens key:                 HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
  Opens key:                 HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
  Opens key:                 HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc-
00aa00404770}\proxystubclsid32
  Opens key:                 HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32
  Opens key:                 HKCU\software\classes\interface\{79eac9c4-baf9-11ce-8c82-
00aa004ba90b}\proxystubclsid32
  Opens key:                 HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32
  Opens key:                 HKCU\software\classes\interface\{000214e6-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                 HKCR\interface\{000214e6-0000-0000-c000-000000000046}\proxystubclsid32
  Opens key:                 HKCU\software\classes\interface\{93f2f68c-1d1b-11d3-a30e-
00c04f79abd1}\proxystubclsid32
  Opens key:                 HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\sxs.dll
  Opens key:                 HKCU\software\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}
  Opens key:                 HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1
  Opens key:                 HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1
  Opens key:                 HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
0000c05bae0b}\1.1\0
  Opens key:                 HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0
  Opens key:                 HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
0000c05bae0b}\1.1\0\win32
  Opens key:                 HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
  Opens key:                 HKLM\software\policies
  Opens key:                 HKCU\software\policies
  Opens key:                 HKCU\software
  Opens key:                 HKLM\software
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\protocoldefaults\
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                 HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                 HKLM\software\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
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\zones\
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
  Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\
  Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
  Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
  Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
  Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
  Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
  Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
```

```
settings\zones\2
  Opens key:               HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
  Opens key:               HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
  Opens key:               HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
  Opens key:               HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
  Opens key:               HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
  Opens key:               HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
  Opens key:               HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
  Opens key:               HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
  Opens key:               HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
  Opens key:               HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
  Opens key:               HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
  Opens key:               HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
  Opens key:               HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
  Opens key:               HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
  Opens key:               HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
  Opens key:               HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
  Opens key:               HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
  Opens key:               HKCR\clsid\{3050f4e1-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:               HKCR\clsid\{3050f4f5-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:               HKCR\clsid\{3050f819-98b5-11cf-bb82-00aa00bdce0b}
  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:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\700aa61e9dbd14abfcc633546a5be910.exe
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{20d04fe0-3aea-1069-
a2d8-08002b30309d}
  Opens key:               HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32
  Opens key:               HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-
11e3-9fc7-806d6172696f}\
  Opens key:               HKCU\software\classes\drive\shellex\folderextensions
  Opens key:               HKCR\drive\shellex\folderextensions
  Opens key:               HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-
4442-804e-409d6c4515e9}
  Opens key:               HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}
  Opens key:               HKCU\software\classes\directory
  Opens key:               HKCR\directory
  Opens key:               HKCU\software\classes\directory\curver
  Opens key:                HKCR\directory\curver
  Opens key:                HKCR\directory\
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\
  Opens key:                HKCU\software\microsoft\windows\currentversion\policies\system
  Opens key:                HKCU\software\classes\directory\shellex\iconhandler
  Opens key:                HKCR\directory\shellex\iconhandler
  Opens key:                HKCU\software\classes\directory\clsid
  Opens key:                HKCR\directory\clsid
  Opens key:                HKCU\software\classes\folder
  Opens key:                HKCR\folder
  Opens key:                HKCU\software\classes\folder\clsid
  Opens key:                HKCR\folder\clsid
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\fileexts
  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\
  Opens key:                HKCU\software\classes\htmlfile\shellex\iconhandler
  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
  Opens key:                HKCU\software\classes\htmlfile\clsid
  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:                HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\implemented
categories\{00021490-0000-0000-c000-000000000046}
  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}
  Opens key:                HKCR\.html\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}
  Opens key:                HKCU\software\classes\systemfileassociations\text\shellex\{a39ee748-
6a27-4817-a6f2-13914bef5890}
  Opens key:                HKCR\systemfileassociations\text\shellex\{a39ee748-6a27-4817-a6f2-
13914bef5890}
  Opens key:                HKCU\software\classes\*
  Opens key:                HKCR\*
  Opens key:                HKCU\software\classes\*\shellex\{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-
000000000046}
  Opens key:                HKCR\htmlfile\shellex\{000214e6-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\.html\shellex\{000214e6-0000-0000-c000-
000000000046}
  Opens key:                HKCR\.html\shellex\{000214e6-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\systemfileassociations\text\shellex\{000214e6-
0000-0000-c000-000000000046}
  Opens key:                HKCR\systemfileassociations\text\shellex\{000214e6-0000-0000-c000-
000000000046}
  Opens key:                HKCU\software\classes\*\shellex\{000214e6-0000-0000-c000-000000000046}
  Opens key:                HKCR\*\shellex\{000214e6-0000-0000-c000-000000000046}
  Opens key:                HKLM\software\policies\microsoft\internet explorer\browseremulation
  Opens key:                HKCU\software\policies\microsoft\internet explorer\browseremulation
  Opens key:                HKLM\software\microsoft\internet explorer\mediatypeclass
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\accepted documents
  Opens key:                HKLM\software\microsoft\windows\currentversion\policies\ratings
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
```

```
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
  Opens key:                HKCU\software\microsoft\internet explorer
  Opens key:                HKLM\software\microsoft\internet explorer
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
  Opens key:                HKCU\software\classes\protocols\name-space handler\file\
  Opens key:                HKCR\protocols\name-space handler\file
  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
  Opens key:                HKCR\protocols\filter\text/html
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject
  Opens key:                HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
  Opens key:                HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
  Opens key:                HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\treatas
  Opens key:                HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas
  Opens key:                HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\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:                HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprochandlerx86
  Opens key:                HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandlerx86
  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
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_aria_support
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_aria_support
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_private_font_setting
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_private_font_setting
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_css_show_hide_events
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_css_show_hide_events
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_expanduri_bypass
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_expanduri_bypass
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
```

```
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
  Opens key:                 HKCU\software\microsoft\windows nt\currentversion\windows
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fls
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fls
  Opens key:                 HKLM\software\microsoft\windows\currentversion\app paths\outlook.exe
  Opens key:                 HKLM\software\microsoft\internet explorer\application compatibility
  Opens key:                 HKLM\software\policies\microsoft\internet explorer\domstorage
  Opens key:                 HKCU\software\policies\microsoft\internet explorer\domstorage
  Opens key:                 HKCU\software\microsoft\internet explorer\domstorage
  Opens key:                 HKLM\software\microsoft\internet explorer\domstorage
  Opens key:                 HKLM\software\policies\microsoft\internet explorer\safety\privacie
  Opens key:                 HKCU\software\policies\microsoft\internet explorer\safety\privacie
  Opens key:                 HKCU\software\microsoft\internet explorer\safety\privacie
  Opens key:                 HKLM\software\microsoft\internet explorer\safety\privacie
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\psapi.dll
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_manage_script_circular_refs
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_manage_script_circular_refs
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload
  Opens key:                 HKLM\software\microsoft\internet explorer\security\floppy access
  Opens key:                 HKCU\software\microsoft\internet explorer\security\adv addrbar spoof
detection
  Opens key:                 HKLM\software\microsoft\internet explorer\security\adv addrbar spoof
detection
  Opens key:                 HKCU\software\classes\protocols\name-space handler\about\
  Opens key:                 HKCR\protocols\name-space handler\about
  Opens key:                 HKCU\software\classes\protocols\handler\about
  Opens key:                 HKCR\protocols\handler\about
  Opens key:                 HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:                 HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:                 HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\treatas
  Opens key:                 HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas
  Opens key:                 HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
  Opens key:                 HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
  Opens key:                 HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserverx86
  Opens key:                 HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86
  Opens key:                 HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\localserver32
  Opens key:                 HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver32
  Opens key:                 HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
  Opens key:                 HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32
  Opens key:                 HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandlerx86
  Opens key:                 HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86
  Opens key:                 HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\localserver
  Opens key:                 HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_document_compatible_mode
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_document_compatible_mode
  Opens key:                 HKLM\software\microsoft\windows\currentversion\internet settings\zones\3
  Opens key:                 HKLM\software\policies\microsoft\internet explorer\zoom
  Opens key:                 HKCU\software\policies\microsoft\internet explorer\zoom
  Opens key:                 HKCU\software\microsoft\internet explorer\zoom
  Opens key:                 HKLM\software\microsoft\internet explorer\zoom
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_weboc_document_zoom
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_weboc_document_zoom
  Opens key:                 HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\progid
  Opens key:                 HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_compat_logging
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_compat_logging
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dlcontrol_behaviors
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dlcontrol_behaviors
  Opens key:                 HKCU\software\policies\microsoft\internet explorer
  Opens key:                 HKLM\software\policies\microsoft\internet explorer\international\scripts
  Opens key:                 HKCU\software\microsoft\internet explorer\international\scripts
  Opens key:                 HKLM\software\microsoft\internet explorer\international\scripts
  Opens key:                 HKLM\software\policies\microsoft\internet explorer\settings
  Opens key:                 HKCU\software\microsoft\internet explorer\settings
  Opens key:                 HKLM\software\microsoft\internet explorer\settings
  Opens key:                 HKCU\software\microsoft\internet explorer\styles
  Opens key:                 HKCU\software\microsoft\windows\currentversion\policies\activedesktop
  Opens key:                 HKCU\software\microsoft\windows\currentversion\policies
  Opens key:                 HKCU\software\microsoft\internet explorer\pagesetup
  Opens key:                 HKCU\software\microsoft\internet explorer\menuext
  Opens key:                 HKCU\software\microsoft\internet explorer\menuext\%s
  Opens key:                 HKLM\system\currentcontrolset\control\nls\codepage
  Opens key:                 HKCU\software\microsoft\internet explorer\international\scripts\3
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\travellog
  Opens key:                 HKLM\software\microsoft\windows\currentversion\explorer\travellog
  Opens key:                 HKLM\software\microsoft\internet explorer\version vector
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_sslux
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_sslux
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
  Opens key:                 HKLM\software\microsoft\windows\currentversion\internet settings\zones\0
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\zones
  Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\
  Opens key:                 HKLM\software\microsoft\windows\currentversion\internet settings\
  Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\
  Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\
  Opens key:                 HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}
  Opens key:                 HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}
  Opens key:                 HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\treatas
  Opens key:                 HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\treatas
  Opens key:                 HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32
  Opens key:                 HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32
  Opens key:                 HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserverx86
  Opens key:                 HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserverx86
  Opens key:                 HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\localserver32
  Opens key:                 HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\localserver32
  Opens key:                 HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
```

```
f4ceaaf59cfc}\inprochandler32
  Opens key:                HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprochandlerx86
  Opens key:                HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-
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 key:                HKLM\software\microsoft\ctf\tip
  Opens key:                HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\languageprofile
  Opens key:                HKCU\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
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}
  Opens key:                HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}
  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
  Opens key:                HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32
  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
  Opens key:                HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver32
  Opens key:                HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprochandler32
  Opens key:                HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprochandlerx86
  Opens key:                HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\localserver
  Opens key:                HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver
  Opens key:                HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}
  Opens key:                HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}
  Opens key:                HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\treatas
  Opens key:                HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\treatas
  Opens key:                HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprocserver32
  Opens key:                HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprocserverx86
  Opens key:                HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\localserver32
  Opens key:                HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\localserver32
  Opens key:                HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprochandler32
  Opens key:                HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprochandlerx86
  Opens key:                HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\localserver
  Opens key:                HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\localserver
  Opens key:                HKLM\software\microsoft\ctf\tip\
  Opens key:                HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
  Opens key:                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
  Opens key:                HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
e988c088ec82}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
  Opens key:                HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
00c04fc324a1}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
  Opens key:                HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-
0f816c09f4ee}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
  Opens key:                HKCU\software\microsoft\ctf\langbaraddin\
  Opens key:                HKLM\software\microsoft\ctf\langbaraddin\
  Opens key:                HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
  Opens key:                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
  Opens key:                HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
```

```
e988c088ec82}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
  Opens key:                HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
00c04fc324a1}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
  Opens key:                HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-
0f816c09f4ee}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
  Opens key:                HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
  Opens key:                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
  Opens key:                HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
  Opens key:                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
  Opens key:                HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
  Opens key:                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
  Opens key:                HKCU\software\policies\microsoft\internet explorer\control panel
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
  Opens key:                HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
  Opens key:                HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
  Opens key:                HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\treatas
  Opens key:                HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\treatas
  Opens key:                HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\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}\inprocserverx86
  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
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547
  Opens key:                HKLM\software\microsoft\internet explorer\activex compatibility
  Opens key:                HKLM\software\microsoft\internet explorer\activex
compatibility\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
  Opens key:                HKLM\system\currentcontrolset\control\nls\locale
  Opens key:                HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
  Opens key:                HKLM\system\currentcontrolset\control\nls\language groups
  Opens key:                HKCU\software\classes\appid\700aa61e9dbd14abfcc633546a5be910.exe
  Opens key:                HKCR\appid\700aa61e9dbd14abfcc633546a5be910.exe
  Opens key:                HKLM\system\currentcontrolset\control\lsa
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\url
history
  Opens key:                HKCU\software\microsoft\ftp
  Opens key:                HKLM\software\policies\microsoft\internet explorer\services
  Opens key:                HKCU\software\microsoft\internet explorer\services
  Opens key:                HKLM\software\microsoft\internet explorer\services
  Opens key:                HKLM\software\policies\microsoft\internet explorer\activities
  Opens key:                HKCU\software\microsoft\internet explorer\activities
  Opens key:                HKLM\software\microsoft\internet explorer\activities
  Opens key:                HKLM\software\policies\microsoft\internet
explorer\infodelivery\restrictions
  Opens key:                HKCU\software\policies\microsoft\internet
explorer\infodelivery\restrictions
  Opens key:                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 key:                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
  Opens key:                HKLM\system\wpa\tabletpc
  Opens key:                HKLM\system\wpa\mediacenter
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\700aa61e9dbd14abfcc633546a5be910.exe
  Opens key:                HKLM\software\policies\microsoft\windows\safer\levelobjects
  Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}
  Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
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:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_leading_file_separator_in_uri_kb933105
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_leading_file_separator_in_uri_kb933105
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
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
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
  Opens key:                HKLM\software\policies\microsoft\internet explorer\dxtrans
  Opens key:                HKCU\software\microsoft\internet explorer\dxtrans
  Opens key:                HKLM\software\microsoft\internet explorer\dxtrans
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
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 key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
  Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
  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\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
  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\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\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}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\localserver
  Opens key:                HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\localserver
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winspool.drv
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iepeers.dll
  Opens key:                HKCU\software\policies\microsoft\internet explorer\persistence
  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
  Opens key:                 HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandler32
  Opens key:                 HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprochandlerx86
  Opens key:                 HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandlerx86
  Opens key:                 HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\localserver
  Opens key:                 HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver
  Opens key:                 HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}
  Opens key:                 HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}
  Opens key:                 HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\treatas
  Opens key:                 HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\treatas
  Opens key:                 HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32
  Opens key:                 HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32
  Opens key:                 HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserverx86
  Opens key:                 HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserverx86
  Opens key:                 HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\localserver32
  Opens key:                 HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver32
  Opens key:                 HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprochandler32
  Opens key:                 HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandler32
  Opens key:                 HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprochandlerx86
  Opens key:                 HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandlerx86
  Opens key:                 HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\localserver
  Opens key:                 HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver
  Opens key:                 HKCU\software\classes\mime\database\content type
  Opens key:                 HKCR\mime\database\content type
  Opens key:                 HKCU\software\classes\mime\database\content type\image/bmp\bits
  Opens key:                 HKCR\mime\database\content type\image/bmp\bits
  Opens key:                 HKCU\software\classes\mime\database\content type\image/gif\bits
  Opens key:                 HKCR\mime\database\content type\image/gif\bits
  Opens key:                 HKCU\software\classes\mime\database\content type\image/jpeg\bits
  Opens key:                 HKCR\mime\database\content type\image/jpeg\bits
  Opens key:                 HKCU\software\classes\mime\database\content type\image/pjpeg\bits
  Opens key:                 HKCR\mime\database\content type\image/pjpeg\bits
  Opens key:                 HKCU\software\classes\mime\database\content type\image/png\bits
  Opens key:                 HKCR\mime\database\content type\image/png\bits
  Opens key:                 HKCU\software\classes\mime\database\content type\image/tiff\bits
  Opens key:                 HKCR\mime\database\content type\image/tiff\bits
  Opens key:                 HKCU\software\classes\mime\database\content type\image/x-icon\bits
  Opens key:                 HKCR\mime\database\content type\image/x-icon\bits
  Opens key:                 HKCU\software\classes\mime\database\content type\image/x-jg\bits
  Opens key:                 HKCR\mime\database\content type\image/x-jg\bits
  Opens key:                 HKCU\software\classes\mime\database\content type\image/x-png\bits
  Opens key:                 HKCR\mime\database\content type\image/x-png\bits
  Opens key:                 HKCU\software\classes\mime\database\content type\image/x-wmf\bits
  Opens key:                 HKCR\mime\database\content type\image/x-wmf\bits
  Opens key:                 HKCU\software\classes\mime\database\content type\image/x-png
  Opens key:                 HKCR\mime\database\content type\image/x-png
  Opens key:                 HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}
  Opens key:                 HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}
  Opens key:                 HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\treatas
  Opens key:                 HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\treatas
  Opens key:                 HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32
  Opens key:                 HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32
  Opens key:                 HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserverx86
  Opens key:                 HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserverx86
  Opens key:                 HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\localserver32
  Opens key:                 HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver32
  Opens key:                 HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprochandler32
  Opens key:                 HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandler32
  Opens key:                 HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprochandlerx86
  Opens key:                 HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandlerx86
  Opens key:                 HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\localserver
  Opens key:                 HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\pngfilt.dll
  Opens key:                 HKCU\software\classes\.gif
  Opens key:                 HKCR\.gif
  Opens key:                 HKLM\software\microsoft\windows\currentversion\internet
```

```
settings\5.0\cache
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
  Opens key:                HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
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}
  Opens key:                HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
e988c088ec82}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
  Opens key:                HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
00c04fc324a1}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
  Opens key:                HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-
0f816c09f4ee}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
  Opens key:                HKCU\software\microsoft\internet
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
  Opens key:                HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}
  Opens key:                HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}
  Opens key:                HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\treatas
  Opens key:                HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\treatas
  Opens key:                HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32
  Opens key:                HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserverx86
  Opens key:                HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\localserver32
  Opens key:                HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\localserver32
  Opens key:                HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprochandler32
  Opens key:                HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprochandlerx86
  Opens key:                HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\localserver
  Opens key:                HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\localserver
  Opens key:                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
  Opens key:                HKLM\software\microsoft\windows\currentversion\controls folder\powercfg
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
  Opens key:                HKLM\software\microsoft\internet
```

```
explorer\main\featurecontrol\feature_bufferbreaking_818408
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
  Opens key:                HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
  Opens key:                 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:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\tapi32.dll
  Opens key:                 HKLM\software\microsoft\windows\currentversion\telephony
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasapi32.dll
  Opens key:                 HKLM\software\microsoft\tracing\rasapi32
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\userenv.dll
  Opens key:                 HKLM\system\currentcontrolset\control\productoptions
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Opens key:                 HKLM\software\policies\microsoft\windows\system
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\profilelist
  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\currentcontrolset\control\securityproviders
  Opens key:                 HKLM\system\currentcontrolset\control\lsa\sspicache
  Opens key:                 HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll
  Opens key:                 HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll
  Opens key:                 HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll
  Opens key:                 HKLM\system\currentcontrolset\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-c000-000000000046}
  Opens key:                 HKCR\clsid\{00021401-0000-0000-c000-000000000046}
  Opens key:                 HKCU\software\classes\clsid\{00021401-0000-0000-c000-
000000000046}\treatas
  Opens key:                 HKCR\clsid\{00021401-0000-0000-c000-000000000046}\treatas
  Opens key:                 HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
  Opens key:                 HKCU\software\classes\clsid\{00021401-0000-0000-c000-
000000000046}\inprocserver32
  Opens key:                 HKCR\clsid\{00021401-0000-0000-c000-000000000046}\inprocserver32
  Opens key:                 HKCU\software\classes\clsid\{00021401-0000-0000-c000-
000000000046}\inprocserverx86
```

```
  Opens key:                HKCR\clsid\{00021401-0000-0000-c000-000000000046}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{00021401-0000-0000-c000-
000000000046}\localserver32
  Opens key:                HKCR\clsid\{00021401-0000-0000-c000-000000000046}\localserver32
  Opens key:                HKCU\software\classes\clsid\{00021401-0000-0000-c000-
000000000046}\inprochandler32
  Opens key:                HKCR\clsid\{00021401-0000-0000-c000-000000000046}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{00021401-0000-0000-c000-
000000000046}\inprochandlerx86
  Opens key:                HKCR\clsid\{00021401-0000-0000-c000-000000000046}\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-c000-000000000046}\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\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  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\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableall]
  Queries value:            HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableallforole32]
  Queries value:            HKCU\control panel\desktop[multiuilanguageid]
  Queries value:            HKCU\control panel\desktop[smoothscroll]
  Queries value:            HKLM\system\setup[systemsetupinprogress]
  Queries 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-
0000-000000000000]
```

```
  Queries value:            HKLM\software\microsoft\ctf\systemshared[cuas]
  Queries value:            HKCU\keyboard layout\toggle[language hotkey]
  Queries value:            HKCU\keyboard layout\toggle[hotkey]
  Queries value:            HKCU\keyboard layout\toggle[layout hotkey]
  Queries value:            HKLM\software\microsoft\ctf[enableanchorcontext]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
  Queries value:            HKCU\software\microsoft\ctf[disable thread input manager]
  Queries value:            HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[enabledhcp]
  Queries 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]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpserver]
  Queries value:            HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
  Queries value:            HKLM\system\wpa\pnp[seed]
  Queries value:            HKLM\system\setup[osloaderpath]
  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]
  Queries 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]
  Queries 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[]
  Queries value:            HKLM\software\microsoft\com3[com+enabled]
  Queries value:            HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
  Queries value:            HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]
  Queries value:            HKLM\software\microsoft\com3[regdbversion]
  Queries value:            HKCR\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32[]
  Queries value:            HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[appid]
  Queries value:            HKCR\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[threadingmodel]
  Queries value:            HKLM\software\microsoft\internet explorer\setup[iexplorelastmodifiedlow]
  Queries value:            HKLM\software\microsoft\internet
explorer\setup[iexplorelastmodifiedhigh]
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  Queries value:            HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib[]
  Queries value:            HKLM\software\microsoft\internet explorer\setup[installstarted]
  Queries value:            HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32[]
  Queries value:            HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32[]
  Queries value:            HKCR\interface\{000214e6-0000-0000-c000-000000000046}\proxystubclsid32[]
  Queries value:            HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32[]
  Queries 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]
  Queries value:            HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[flags]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[flags]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[flags]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
```

```
settings[enablepunycode]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonethood]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
  Queries value:            HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-
11e3-9fc7-806d6172696f}[data]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-
11e3-9fc7-806d6172696f}[generation]
  Queries value:            HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[forceactivedesktopon]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
  Queries value:            HKCR\directory[docobject]
  Queries value:            HKCR\directory[browseinplace]
  Queries value:            HKCR\directory[isshortcut]
  Queries value:            HKCR\directory[alwaysshowext]
  Queries value:            HKCR\directory[nevershowext]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.html[progid]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.html[application]
  Queries value:            HKCR\.html[]
  Queries value:            HKCR\htmlfile\shellex\iconhandler[]
  Queries value:            HKCR\htmlfile[docobject]
  Queries value:            HKCR\.html[perceivedtype]
  Queries value:            HKCR\systemfileassociations\text[docobject]
  Queries value:            HKCR\htmlfile[browseinplace]
  Queries value:            HKCR\systemfileassociations\text[browseinplace]
  Queries value:            HKCR\htmlfile\clsid[]
  Queries value:            HKCR\htmlfile[isshortcut]
  Queries value:            HKCR\systemfileassociations\text[isshortcut]
  Queries value:            HKCR\htmlfile[alwaysshowext]
  Queries value:             HKCR\systemfileassociations\text[alwaysshowext]
  Queries value:             HKCR\htmlfile[nevershowext]
  Queries value:             HKCR\systemfileassociations\text[nevershowext]
  Queries value:             HKCU\software\microsoft\internet explorer\main[frametabwindow]
  Queries value:             HKLM\software\microsoft\internet explorer\main[frametabwindow]
  Queries value:             HKCU\software\microsoft\internet explorer\main[framemerging]
  Queries value:             HKLM\software\microsoft\internet explorer\main[framemerging]
  Queries value:             HKCU\software\microsoft\internet explorer\main[sessionmerging]
  Queries value:             HKLM\software\microsoft\internet explorer\main[sessionmerging]
  Queries value:             HKCU\software\microsoft\internet explorer\main[admintabprocs]
  Queries value:             HKLM\software\microsoft\internet explorer\main[admintabprocs]
  Queries value:             HKLM\software\policies\microsoft\internet explorer\main[tabprocgrowth]
  Queries value:             HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
  Queries value:             HKLM\software\microsoft\internet explorer\main[tabprocgrowth]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nofileurl]
  Queries value:             HKLM\software\microsoft\internet explorer\main[navigationdelay]
  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]
  Queries value:             HKLM\software\microsoft\windows\currentversion\policies\ratings[key]
  Queries value:             HKCU\software\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
  Queries value:             HKLM\software\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
  Queries value:             HKCU\software\microsoft\internet explorer[no3dborder]
  Queries value:             HKLM\software\microsoft\internet explorer[no3dborder]
  Queries value:             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[700aa61e9dbd14abfcc633546a5be910.exe]
  Queries value:             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[*]
  Queries value:             HKLM\software\microsoft\ole[maximumallowedallocationsize]
  Queries value:             HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
  Queries value:             HKCR\.html[content type]
  Queries value:             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing[700aa61e9dbd14abfcc633546a5be910.exe]
  Queries value:             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing[*]
  Queries value:             HKCU\software\microsoft\windows\currentversion\internet
settings[istextplainhonored]
  Queries value:             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[700aa61e9dbd14abfcc633546a5be910.exe]
  Queries value:             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[*]
  Queries value:             HKCR\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32[inprocserver32]
  Queries value:             HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[]
  Queries value:             HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[appid]
  Queries value:             HKCR\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32[threadingmodel]
  Queries value:             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[700aa61e9dbd14abfcc633546a5be910.exe]
  Queries value:             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[*]
  Queries value:             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching[700aa61e9dbd14abfcc633546a5be910.exe]
  Queries value:             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching[*]
  Queries value:             HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
  Queries value:             HKLM\software\microsoft\internet explorer\application
compatibility[700aa61e9dbd14abfcc633546a5be910.exe]
  Queries value:             HKCU\software\microsoft\internet explorer\domstorage[totallimit]
  Queries value:             HKCU\software\microsoft\internet explorer\domstorage[domainlimit]
  Queries value:             HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinset]
  Queries value:             HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrolldelay]
  Queries value:             HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinterval]
  Queries value:             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[700aa61e9dbd14abfcc633546a5be910.exe]
  Queries value:             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[*]
  Queries value:             HKCR\protocols\handler\about[clsid]
  Queries value:             HKCR\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[inprocserver32]
```

```
  Queries value:             HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
  Queries value:             HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}[appid]
  Queries value:             HKCR\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
  Queries value:             HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2106]
  Queries value:             HKLM\software\microsoft\windows\currentversion\internet
settings\zones\3[2106]
  Queries value:             HKCU\software\microsoft\internet explorer\zoom[zoomdisabled]
  Queries value:             HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[]
  Queries value:             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]
  Queries value:             HKCU\software\microsoft\internet explorer[smartdithering]
  Queries value:             HKCU\software\microsoft\internet explorer[rtfconverterflags]
  Queries value:             HKLM\software\policies\microsoft\internet explorer\main[usecleartype]
  Queries value:             HKCU\software\microsoft\internet explorer\main[usecleartype]
  Queries value:             HKLM\software\policies\microsoft\internet
explorer\main[page_transitions]
  Queries value:             HKCU\software\microsoft\internet explorer\main[page_transitions]
  Queries value:             HKLM\software\policies\microsoft\internet
explorer\main[use_dlgbox_colors]
  Queries value:             HKCU\software\microsoft\internet explorer\main[use_dlgbox_colors]
  Queries value:             HKLM\software\policies\microsoft\internet explorer\main[anchor
underline]
  Queries value:             HKCU\software\microsoft\internet explorer\main[anchor underline]
  Queries value:             HKCU\software\microsoft\internet explorer\main[css_compat]
  Queries value:             HKCU\software\microsoft\internet explorer\main[expand alt text]
  Queries value:             HKLM\software\policies\microsoft\internet explorer\main[display inline
images]
  Queries value:             HKCU\software\microsoft\internet explorer\main[display inline images]
  Queries value:             HKLM\software\policies\microsoft\internet explorer\main[display inline
videos]
  Queries value:             HKCU\software\microsoft\internet explorer\main[display inline videos]
  Queries value:             HKLM\software\policies\microsoft\internet
explorer\main[play_background_sounds]
  Queries value:             HKCU\software\microsoft\internet explorer\main[play_background_sounds]
  Queries value:             HKLM\software\policies\microsoft\internet explorer\main[play_animations]
  Queries value:             HKCU\software\microsoft\internet explorer\main[play_animations]
  Queries value:             HKLM\software\policies\microsoft\internet
explorer\main[print_background]
  Queries value:             HKCU\software\microsoft\internet explorer\main[print_background]
  Queries value:             HKCU\software\microsoft\internet explorer\main[use stylesheets]
  Queries value:             HKLM\software\policies\microsoft\internet explorer\main[smoothscroll]
  Queries value:             HKCU\software\microsoft\internet explorer\main[smoothscroll]
  Queries value:             HKLM\software\policies\microsoft\internet explorer\main[xmlhttp]
  Queries value:             HKCU\software\microsoft\internet explorer\main[xmlhttp]
  Queries value:             HKLM\software\policies\microsoft\internet explorer\main[show image
placeholders]
  Queries value:             HKCU\software\microsoft\internet explorer\main[show image placeholders]
  Queries value:             HKLM\software\policies\microsoft\internet explorer\main[disable script
debugger]
  Queries value:             HKCU\software\microsoft\internet explorer\main[disable script debugger]
  Queries value:             HKCU\software\microsoft\internet explorer\main[disablescriptdebuggerie]
  Queries value:             HKCU\software\microsoft\internet explorer\main[move system caret]
  Queries value:             HKCU\software\microsoft\internet explorer\main[force offscreen
composition]
  Queries value:             HKLM\software\policies\microsoft\internet explorer\main[enable
autoimageresize]
  Queries value:             HKCU\software\microsoft\internet explorer\main[enable autoimageresize]
  Queries value:             HKCU\software\microsoft\internet explorer\main[usethemes]
  Queries value:             HKCU\software\microsoft\internet explorer\main[usehr]
  Queries value:             HKCU\software\microsoft\internet explorer\main[q300829]
  Queries value:             HKCU\software\microsoft\internet explorer\main[cleanup htcs]
  Queries value:             HKLM\software\policies\microsoft\internet explorer\main[xdomainrequest]
  Queries value:             HKCU\software\microsoft\internet explorer\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]
  Queries value:             HKLM\software\microsoft\internet explorer\main[domstorage]
  Queries value:             HKCU\software\microsoft\internet
explorer\international[default_codepage]
  Queries value:             HKCU\software\microsoft\internet explorer\international[autodetect]
  Queries value:             HKCU\software\microsoft\internet
explorer\international\scripts[default_iefontsizeprivate]
  Queries value:             HKCU\software\microsoft\internet explorer\settings[anchor color]
  Queries value:             HKCU\software\microsoft\internet explorer\settings[anchor color visited]
  Queries value:             HKCU\software\microsoft\internet explorer\settings[anchor color hover]
  Queries value:             HKCU\software\microsoft\internet explorer\settings[always use my colors]
  Queries value:             HKCU\software\microsoft\internet explorer\settings[always use my font
size]
```

```
  Queries value:            HKCU\software\microsoft\internet explorer\settings[always use my font
face]
  Queries value:            HKCU\software\microsoft\internet explorer\settings[disable visited
hyperlinks]
  Queries value:            HKCU\software\microsoft\internet explorer\settings[use anchor hover
color]
  Queries value:            HKCU\software\microsoft\internet explorer\settings[miscflags]
  Queries value:            HKCU\software\microsoft\windows\currentversion\policies[allow
programmatic cut_copy_paste]
  Queries value:            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[*]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
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]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
  Queries value:            HKCR\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32[]
  Queries value:            HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[appid]
  Queries value:            HKCR\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[threadingmodel]
  Queries value:            HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}[enable]
  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:            HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}[description]
  Queries value:            HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[description]
  Queries value:            HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}[description]
  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]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
```

```
settings\zones\0[1201]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Queries value:            HKLM\system\currentcontrolset\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\policies\microsoft\windows\safer\codeidentifiers\0\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:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemdata]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[hashalg]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemsize]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[saferflags]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[itemdata]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[hashalg]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[itemsize]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[saferflags]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemdata]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[hashalg]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemsize]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[saferflags]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemdata]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\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\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[hashalg]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemsize]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[saferflags]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemdata]
```

```
  Queries value:            HKCR\.css[content type]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[hashalg]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemsize]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[saferflags]
  Queries value:            HKLM\software\microsoft\internet explorer\default behaviors[discovery]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
  Queries value:            HKCR\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
  Queries value:            HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}[appid]
  Queries value:            HKCR\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
  Queries value:            HKCR\.png[content type]
  Queries value:            HKCR\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[]
  Queries value:            HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}[appid]
  Queries value:            HKCR\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[threadingmodel]
  Queries value:            HKCR\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32[]
  Queries value:            HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}[appid]
  Queries value:            HKCR\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32[threadingmodel]
  Queries value:            HKCR\mime\database\content type\image/bmp\bits[0]
  Queries value:            HKCR\mime\database\content type\image/gif\bits[0]
  Queries value:            HKCR\mime\database\content type\image/jpeg\bits[0]
  Queries value:            HKCR\mime\database\content type\image/pjpeg\bits[0]
  Queries value:            HKCR\mime\database\content type\image/png\bits[0]
  Queries value:            HKCR\mime\database\content type\image/x-png\bits[0]
  Queries value:            HKCR\mime\database\content type\image/x-wmf\bits[0]
  Queries value:            HKCR\mime\database\content type\image/x-png[image filter clsid]
  Queries value:            HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[]
  Queries value:            HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}[appid]
  Queries value:            HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32[threadingmodel]
  Queries value:            HKCR\.gif[content type]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[signature]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cacheprefix]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cachelimit]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cachelimit]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
```

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

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

```
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[700aa61e9dbd14abfcc633546a5be910.exe]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disablent4rascheck]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[bypassftptimecheck]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduringauth]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertsending]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
```

```
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[urlencoding]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[truncatefilename]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[badproxyexpirestime]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
  Queries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
  Queries 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]
  Queries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32maxnumrequestretries]
  Queries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32requestretrytimeout]
  Queries value:            HKLM\software\microsoft\tracing[enableconsoletracing]
  Queries value:            HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
  Queries value:            HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
  Queries value:            HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
  Queries value:            HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
  Queries value:            HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
  Queries value:            HKLM\software\microsoft\tracing\rasapi32[filedirectory]
  Queries value:            HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common appdata]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\winlogon[chkaccdebuglevel]
  Queries value:            HKLM\system\currentcontrolset\control\productoptions[producttype]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[personal]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local settings]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\winlogon[rsopdebuglevel]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\profilelist[profilesdirectory]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\profilelist[allusersprofile]
```

```
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\profilelist[defaultuserprofile]
  Queries value:              HKLM\software\microsoft\windows\currentversion[programfilesdir]
  Queries value:              HKLM\software\microsoft\windows\currentversion[commonfilesdir]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[profileimagepath]
  Queries value:              HKCU\software\microsoft\windows
nt\currentversion\winlogon[parseautoexec]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
  Queries value:              HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
```

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

```
  Queries value:          HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]
  Queries value:          HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]
  Queries value:          HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities]
  Queries value:          HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid]
  Queries value:          HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version]
  Queries value:          HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize]
  Queries value:          HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name]
  Queries value:          HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities]
  Queries value:          HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid]
  Queries value:          HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version]
  Queries value:          HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize]
  Queries value:          HKLM\software\microsoft\cryptography[machineguid]
  Queries value:          HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[desktop]
  Queries value:          HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
  Queries value:          HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Queries value:          HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
  Queries value:          HKCR\clsid\{00021401-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
  Queries value:          HKCR\clsid\{00021401-0000-0000-c000-000000000046}\inprocserver32[]
  Queries value:          HKCR\clsid\{00021401-0000-0000-c000-000000000046}[appid]
  Queries value:          HKCR\clsid\{00021401-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[comparejunctionness]
  Queries value:          HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common documents]
  Queries value:          HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common desktop]
  Queries value:          HKCR\.exe[]
  Queries value:          HKCR\exefile[docobject]
  Queries value:          HKCR\exefile[browseinplace]
  Queries value:          HKCR\exefile[isshortcut]
  Queries value:          HKCR\exefile[alwaysshowext]
  Queries value:          HKCR\exefile[nevershowext]
  Queries value:          HKCR\network\sharinghandler[]
  Queries value:
HKLM\system\currentcontrolset\services\lanmanserver\defaultsecurity[srvsvcdefaultshareinfo]
  Queries value:          HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[start menu]
  Queries value:          HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common start menu]
  Queries value:          HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[my pictures]
  Queries value:          HKLM\software\microsoft\windows\currentversion[programfilesdir (x86)]
  Queries value:          HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[commonpictures]
  Queries value:          HKCR\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\inprocserver32[]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[noshareddocuments]
  Queries value:          HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[commonmusic]
  Queries value:          HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[commonvideo]
  Queries value:          HKLM\software\microsoft\internet explorer\main[maxrenderline]
  Value changes:          HKLM\software\microsoft\cryptography\rng[seed]
  Value changes:          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[proxybypass]
  Value changes:          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[intranetname]
  Value changes:          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[uncasintranet]
  Value changes:          HKCU\software\microsoft\windows\currentversion\internet
```

```
settings\zonemap[autodetect]
  Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-
806d6172696f}[baseclass]
  Value changes:             HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
  Value changes:             HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cookies]
  Value changes:             HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[history]
  Value changes:             HKCU\software\microsoft\windows\currentversion\explorer\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]
```