Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details Host: mag2, Sample ID: 11, Task ID: 42

Task ID: 42 Risk Level:

Date Processed: 2016-04-28 12:47:00 (UTC)

Processing Time: 61.11 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe"

Sample ID: 11 Type: basic Owner: admin

83497c45d30bcb551f5f55f3f63b6fa1 Label: 2016-04-28 12:44:50 (UTC)

Date Added: PE32:win32:gui File Type:

File Size: 892928 bytes

83497c45d30bcb551f5f55f3f63b6fa1 MD5:

SHA256: 40932ac88b750f1f3077f2e50d9184de1c3b4914e92ceb64cfc4638c3d91ee14

Description: None

Pattern Matching Results

3 Long sleep detected

3 Connects to local host

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

4 Checks whether debugger is present

Process/Thread Events

C:\WINDOWS\Temp\83497c45d30bcb551f5f55f3f63b6fa1.exe Creates process:

["c:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe"]

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

Named Object Events

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

1957994488-1003

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

1957994488-1003

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

1957994488-1003

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

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

1957994488-1003

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

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

settings!temporary internet files!content.ie5!

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

settings!history!history.ie5!

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

Creates mutex: $\verb|\BaseNamedObjects\ZonesCounterMutex| \\$

Creates mutex: \BaseNamedObjects\ZoneAttributeCacheCounterMutex

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

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

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

Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1} Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}

File System Events

Creates

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

Files\Content.IE5\QXMNQBKF\104[1]

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

Files\Content.IE5\CXCXW1MR\property_front[1].aspx

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

Files\Content.IE5\CXCXW1MR\JMX.Frame.Common[1].js

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

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

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

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

C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\jquery-1.4.2.min[1].js

C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\client_ending[1].htm

```
C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\QXMNQBKF\SRO-ending[1].jpg
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\QXMNQBKF\btn_facebook[1].jpg
 Opens:
                         C:\Documents and Settings\Admin
 Opens:
                         C:\WINDOWS\system32\winspool.drv
                         C:\WINDOWS\system32\oledlg.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\imm32.dll
 Opens:
                         C:\WINDOWS\system32\comctl32.dll
                         C:\WINDOWS\system32\COMCTL32.dll.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\COMCTL32.dll.124.Config
 Opens:
                         C:\WINDOWS\system32\shell32.dll
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Manifest
                         C:\WINDOWS\system32\SHELL32.dll.124.Config
 Opens:
 Opens:
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
 Opens:
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
 Opens:
                         C:\WINDOWS\WindowsShell.Manifest
                         C:\WINDOWS\WindowsShell.Config
 Opens:
                         C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe.2.Manifest
 Opens:
                         C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe.3.Manifest
 Opens:
 Opens:
                         C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe.Manifest
 Opens:
                         C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe.Config
 Opens:
                         C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe.1000.Manifest
                         C:\WINDOWS\system32\MSCTF.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\MSCTFIME.IME
 Opens:
                         C:\WINDOWS\winhlp32.exe
                         C:\WINDOWS\system32\rpcss.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\clbcatq.dll
 Opens:
                         C:\WINDOWS\system32\comres.dll
                         C:\WINDOWS\Registration\R00000000007.clb
 Opens:
 Opens:
                         C:\WINDOWS\system32\ieframe.dll
 Opens:
                         C:\Program Files\Internet Explorer\iexplore.exe
 Opens:
                         C:\WINDOWS\system32\ieframe.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\ieframe.dll.123.Config
 Opens:
                         C:\WINDOWS\system32\en-US\ieframe.dll.mui
 Opens:
                         C:\WINDOWS\system32\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:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5
                         C:\Documents and Settings\Admin\Local Settings\History
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History\History.IE5
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\index.dat
                         C:\Documents and Settings\Admin\Cookies
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Cookies\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\index.dat
                         C:\WINDOWS\system32\ws2_32.dll
 Opens:
                         C:\WINDOWS\system32\ws2help.dll
 Opens:
 Opens:
                         C:\WINDOWS\svstem32\mshtml.dll
 Opens:
                         C:\WINDOWS\system32\msls31.dll
 Opens:
                         C:\
 Opens:
                         C:\WINDOWS
                         C:\WINDOWS\Temp\c439f45c-fd60-4bae-ac49-f0e988e69cc9
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF
                         C:\WINDOWS\system32\psapi.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\mlang.dll
 Opens:
                         C:\WINDOWS\system32\MLANG.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\MLANG.dll.123.Config
 Opens:
                         C:\WINDOWS\system32\MSIMTF.dll
 Opens:
                         C:\WINDOWS\system32\rasapi32.dll
 Opens:
                         C:\WINDOWS\system32\rasman.dll
 Opens:
                         C:\WINDOWS\system32\netapi32.dll
 Opens:
                         C:\WINDOWS\system32\tapi32.dll
                         C:\WINDOWS\system32\rtutils.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\winmm.dll
 Opens:
                         C:\WINDOWS\system32\TAPI32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\TAPI32.dll.124.Config
 Opens:
                         C:\AUTOEXEC.BAT
                         C:\Documents and Settings\All Users\Application
 Opens:
Data\Microsoft\Network\Connections\Pbk
                         C:\WINDOWS\system32\ras
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\Network\Connections\Pbk\
 Opens:
                         C:\WINDOWS\system32\sensapi.dll
                         C:\WINDOWS\svstem32\mswsock.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\hnetcfg.dll
```

```
C:\WINDOWS\system32\wshtcpip.dll
 Opens:
 Opens:
                         C:\WINDOWS\Fonts\times.ttf
 Opens:
                         C:\WINDOWS\system32\msv1_0.dll
                         C:\WINDOWS\system32\iphlpapi.dll
 Opens:
                         C:\WINDOWS\system32\rasadhlp.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\dnsapi.dll
 Opens:
                         C:\WINDOWS\system32\drivers\etc\hosts
                         C:\WINDOWS\system32\rsaenh.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\crypt32.dll
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\property_front[1].aspx
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\JMX.Frame.Common[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF\JMX_FormValidator[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\UH4D6D6X\jquery-1.4.2.min[1].js
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\JMX_AjaxControl[1].js
                         C:\WINDOWS\system32\jscript.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\winlogon.exe
 Opens:
                         C:\WINDOWS\system32\xpsp2res.dll
                         C:\WINDOWS\system32\en-US\jscript.dll.mui
 Opens:
 Opens:
                         C:\WINDOWS\system32\uxtheme.dll
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files \verb|\| Content.IE5 \verb|\| CXCXW1MR \verb|\| client_ending[1].htm \\
                         C:\Documents and Settings\Admin\IETldCache
                         C:\Documents and Settings\Admin\IETldCache\index.dat
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Opens:
Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\QXMNQBKF\104[1]
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\property front[1].aspx
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\CXCXW1MR\JMX.Frame.Common[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\QXMNQBKF\JMX_FormValidator[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\JMX_AjaxControl[1].js
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\jquery-1.4.2.min[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\CXCXW1MR\client_ending[1].htm
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\SRO-ending[1].jpg
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\btn_facebook[1].jpg
                         C:\WINDOWS\Registration\R00000000007.clb
 Reads from:
 Reads from:
                         C:\AUTOEXEC.BAT
 Reads from:
                         C:\WINDOWS\system32\drivers\etc\hosts
 Reads from:
                         C:\WINDOWS\system32\rsaenh.dll
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\jquery-1.4.2.min[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\QXMNQBKF\JMX_FormValidator[1].js
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\JMX_AjaxControl[1].js
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Reads from:
Files\Content.IE5\CXCXW1MR\JMX.Frame.Common[1].js
```

Network Events

DNS query:	www.joymax.com
DNS query:	file.joymax.com
DNS query:	silkroadcp.joymax.com
DNS query:	img.joymax.com
DNS response:	www.joymax.com ⇒ 222.111.176.232
DNS response:	file.joymax.com ⇒ 222.111.176.232
DNS response:	silkroadcp.joymax.com ⇒ 121.128.133.11
DNS response:	silkroadcp.joymax.com ⇒ 121.128.133.12
DNS response:	img.joymax.com.gccdn.net ⇒ 14.0.55.3
DNS response:	img.joymax.com.gccdn.net ⇒ 14.0.55.10
Connects to:	127.0.0.1:1047
Connects to:	222.111.176.232:80
Connects to:	121.128.133.11:80
Connects to:	14.0.55.3:80
Sends data to:	8.8.8.53
Sends data to:	127.0.0.1:1047
Sends data to:	file.joymax.com:80 (222.111.176.232)
Sends data to:	silkroadcp.joymax.com:80 (121.128.133.11)
Sends data to:	img.joymax.com.gccdn.net:80 (14.0.55.3)
Receives data from:	0.0.0.0:0

Receives data from: 127.0.0.1:1047

file.joymax.com:80 (222.111.176.232) Receives data from: Receives data from:

Windows Registry Events

silkroadcp.joymax.com:80 (121.128.133.11) Receives data from: img.joymax.com.gccdn.net:80 (14.0.55.3) Creates key: HKLM\software\microsoft\windows\currentversion\shell extensions\blocked Creates key: HKCU\software\microsoft\windows\currentversion\shell extensions\blocked Creates key: HKLM\software\microsoft\windows\currentversion\shell extensions\cached Creates key: $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \shell extensions \cached$ Creates kev: HKCU\software\microsoft\windows\currentversion\internet settings Creates key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders Creates kev: HKCU\software\microsoft\windows\currentversion\explorer\shell folders Creates kev: HKLM\software\microsoft\tracing HKLM\software\microsoft\windows\currentversion\explorer\user shell Creates key: folders Creates key: $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows nt\- current version\+ winlogon$ 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 Creates key: $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ settings\p3p\history HKCU\software\microsoft\windows script\settings Creates key: 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\83497c45d30bcb551f5f55f3f63b6fa1.exe Opens key: HKLM\system\currentcontrolset\control\terminal server 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\gdi32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: HKLM\system\currentcontrolset\control\session manager 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\user32.dll

options\kernel32.dll

Opens key: options\secur32.dll

Opens key: options\rpcrt4.dll Opens key:

options\advapi32.dll Opens key:

options\comctl32.dll Opens key:

options\msvcrt.dll Opens key: options\shlwapi.dll

Opens key:

options\shell32.dll Opens key:

options\comdlg32.dll Opens key:

options\winspool.drv

Opens key: options\ole32.dll Opens key: options\oledlg.dll Opens key:

options\oleaut32.dll

Opens key: Opens key: Opens key: Opens key: Opens key: Opens key:

Opens key:

Opens key:

HKLM\system\currentcontrolset\control\error message instrument\ HKLM\svstem\currentcontrolset\control\error message instrument HKLM\software\microsoft\windows nt\currentversion\gre_initialize HKLM\software\microsoft\windows nt\currentversion\compatibility32 HKLM\software\microsoft\windows nt\currentversion\ime compatibility $\label{lem:hklm} \mbox{HKLM} \mbox{$\tt MKLM} \mbox$ $\label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + nt + current + version + winlog on + current + version + version$ HKLM\

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

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

Opens key: HKCU\

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

Opens key: HKCU\control panel\desktop

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

Opens key: HKLM\system\setup

Opens key:

 $HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \mbox{\current} version \label{lem:hklm} idebyside \label{lem:hklm} \label{lkm} \label{lkm}$

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

Opens key: HKLM\software\microsoft\ole

Opens key: HKCR\interface

Opens key: HKCR\interface\{00020400-0000-0000-c000-00000000046}

HKCU\software\classes\ Opens key: Opens key: HKCU\software\classes\clsid Opens key: HKCR\clsid HKLM\software\microsoft\oleaut Opens kev: Opens key: HKLM\software\microsoft\oleaut\userera

Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer Opens key: HKCU\software\microsoft\windows\currentversion\policies\network Opens key: HKCU\software\microsoft\windows\currentversion\policies\comdlg32 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msctf.dll

Opens key:

HKLM\software\microsoft\ctf\compatibility\83497c45d30bcb551f5f55f3f63b6fa1.exe

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

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

HKI M\software\microsoft\windows nt\currentversion\imm Opens key:

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

options\version.dll

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

options\msctfime.ime

HKCU\software\microsoft\ctf Opens key:

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

Opens key: HKLM\software\microsoft\com3

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

options\comres.dll

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

options\clbcatq.dll

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

HKLM\software\classes Opens kev:

HKII\ Opens key:

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

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

00c04fd705a2}\treatas

HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas Opens kev: Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32

Opens kev:

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

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

00c04fd705a2}\inprocserverx86

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

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

00c04fd705a2}\localserver32

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

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

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

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

00c04fd705a2}\localserver

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

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

options\iertutil.dll

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

Opens key: HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe Opens key: HKLM\software\microsoft\internet explorer\setup Opens key: HKLM\system\currentcontrolset\control\wmi\security HKCU\software\classes\interface\{eab22ac1-30c1-11cf-a7eb-

Opens key: 0000c05bae0b}\typelib

Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{a4a1a128-768f-41e0-bf75-e4fddd701cba\}$

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

00aa00404770}\proxystubclsid32

Opens key:

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

00aa004ba90b}\proxystubclsid32 HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32 Opens kev: HKCU\software\classes\interface\{000214e6-0000-0000-c000-Opens kev: 00000000046}\proxystubclsid32 Opens key: HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32 Opens key: HKCU\software\classes\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32 HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32 Opens key: Opens key: HKLM\software\microsoft\rpc\pagedbuffers HKLM\software\microsoft\rpc Opens key: Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution options\83497c45d30bcb551f5f55f3f63b6fa1.exe\rpcthreadpoolthrottle Opens key: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKLM\system\currentcontrolset\control\computername Opens key: $HKLM \verb|\system| current controlset| \verb|\computername| active computername|$ Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\urlmon.dll Opens key: HKCU\software\classes\protocols\name-space handler\ Opens key: HKCR\protocols\name-space handler HKCU\software\classes\protocols\name-space handler Opens key: Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings HKLM\software\microsoft\windows\currentversion\internet settings Opens kev: Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_protocol_lockdown Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\ HKLM\software\policies\microsoft\internet explorer\main\featurecontrol Opens key: Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\internet explorer\mbox{\tt main\feature} control} \\$ Opens key: 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: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}$ settings\zonemap\domains\ HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zonemap\ranges\ HKCU\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zonemap\ranges\ Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_unc_savedfilecheck HKCU\software\microsoft\windows\currentversion\internet settings Opens key: Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_http_username_password_disable Opens kev: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_http_username_password_disable HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562 Opens key: HKCU\software\microsoft\internet explorer\main Opens key: HKLM\software\microsoft\internet explorer\main Opens key: HKLM\software\policies\microsoft\internet explorer\main Opens key: HKCU\software\policies\microsoft\internet explorer\main Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer Opens key: $HKLM \ software \ `microsoft \ 'windows \ 'current version' shell compatibility \ 'applications' \ 83497c45d30bcb551f5f55f3f63b6fa1.exe$ Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{871c5380-42a0-1069a2ea-08002b30309d} $HKCU \setminus software \setminus classes \setminus clsid \setminus \{871c5380-42a0-1069-a2ea-1060-a2ea-106$ Opens key: 08002b30309d}\inprocserver32 Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\apphelp.dll

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

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

08002b30309d}\treatas

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

08002b30309d}\inprocserverx86

 $\label{local-eq:hkcr} $$ HKCR\clsid_{871c5380-42a0-1069-a2ea-08002b30309d} \in \clsid_{871c5380-42a0-1069-a2ea-08002b30309d} $$ inprocessor (a) $$ $$ in $$ (a) $$ in $$ (b) $$ in $$ (b) $$ in $$ (b) $$ (b) $$ (c) $$ (c)$ Opens key:

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

08002b30309d}\localserver32

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

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

08002b30309d}\inprochandler32

 $\label{lem:hkcr} $$HKCR\clsid{871c5380-42a0-1069-a2ea-08002b30309d} \in \clsid{871c5380-42a0-1069-a2ea-08002b30309d} in prochandler 32 and $$A$ (a) $$A$ (b) $$A$ (b) $$A$ (c) $$A$ (c)$ Opens key:

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

08002b30309d}\inprochandlerx86

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

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

08002b30309d}\localserver

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

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

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

options\normaliz.dll

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

options\wininet.dll

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

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

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

settings\5.0\cache

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

settings\5.0\cache

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

settings\5.0\cache\content

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

settings\5.0\cache\content

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

settings\5.0\cache\cookies

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

settings\5.0\cache\cookies

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

settings\5.0\cache\history

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

settings\5.0\cache\history Opens kev:

HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache

HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\extensible cache\domstore

Opens key:

HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat

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

settings\5.0\cache\extensible cache\iecompat

HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\extensible cache\ietld

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

settings\5.0\cache\extensible cache\mshist012014033120140407

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

settings\5.0\cache\extensible cache\mshist012014041220140413

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

settings\5.0\cache\extensible cache\privacie:

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset

HKCU\software\microsoft\internet Opens key: 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

HKCU\software\microsoft\internet Opens key: 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
                    HKLM\software\microsoft\internet
 Opens kev:
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
                   HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                    HKLM\software\microsoft\internet
 Opens key:
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
                    HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
 Opens key:
                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
                    HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\ws2_32.dll
 Opens key:
                    HKLM\system\currentcontrolset\services\winsock2\parameters
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries
 Opens key:
Opens kev:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
 Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000005
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
 Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000001
 Opens key:
Opens kev:
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 kev:
                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature return failed connect content kb942615
 Opens key:
                    HKLM\software\policies\microsoft\internet explorer\browseremulation
 Opens key:
                    HKCU\software\policies\microsoft\internet explorer\browseremulation
 Opens key:
                    HKCU\software\classes\protocols\name-space handler\res\
 Opens key:
                    HKCR\protocols\name-space handler\res
```

Opens key: HKCU\software\classes\protocols\name-space handler*\ Opens key: HKCR\protocols\name-space handler* ${\tt HKCU \ software \ classes \ protocols \ handler \ res}$ Opens kev: HKCR\protocols\handler\res Opens key: Opens kev: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b} $HKCR \verb|\clsid|{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}|$ Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\treatas HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\treatas Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\inprocserver32 $HKCR \verb|\clsid|{3050f3bc-98b5-11cf-bb82-00aa00bdce0b} \verb|\inprocserver32|$ Opens key: Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86 Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86 HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\localserver32 Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\localserver32 Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32 Opens key: $HKCR \clsid \ \{3050f3bc-98b5-11cf-bb82-00aa00bdce0b\} \ \ in prochandler 32$ HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\inprochandlerx86 Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86 Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\localserver Opens key: $HKCR \verb|\clsid|{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\\ \\ local server$ 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 HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120 HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131 HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_aria_support HKLM\software\microsoft\internet Opens key: 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 HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_allow_expanduri_bypass Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_allow_expanduri_bypass HKCU\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245 HKLM\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_databinding_support HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_databinding_support Opens kev: 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 kev: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_enable_dynamic_object_caching Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_object_caching HKLM\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_object_caching

```
Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
                          HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
 Opens key:
                          HKCU\software\microsoft\windows nt\currentversion\windows
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fls
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fls
                          HKLM\software\microsoft\windows\currentversion\app paths\outlook.exe
 Opens key:
 Opens key:
                          HKLM\software\microsoft\internet explorer\application compatibility
 Opens key:
                          HKLM\software\policies\microsoft\internet explorer\domstorage
                          HKCU\software\policies\microsoft\internet explorer\domstorage
 Opens kev:
 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 kev:
                          HKLM\software\microsoft\internet explorer\safety\privacie
 Opens key:
                          HKLM\software\microsoft\internet explorer\mediatypeclass
 Opens key:
                          HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\accepted documents
 Opens key:
                          HKLM\software\microsoft\windows\currentversion\policies\ratings
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
                          HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\zonemap\protocoldefaults\
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\zonemap\domains\
                          HKLM\software\microsoft\windows\currentversion\internet
 Opens key:
settings\zonemap\domains\
                          HKLM\software\microsoft\windows\currentversion\internet
 Opens key:
settings\zonemap\domains\msn.com
 Opens key:
                          \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
settings\zonemap\domains\msn.com\related
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
                          HKCU\software\microsoft\internet explorer\ietld
 Opens key:
                          HKLM\software\policies\microsoft\internet explorer\security
 Opens key:
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\
                          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:
 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 kev:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
 Opens key:
                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} internet \end{tabular}
settings\zones\0
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\zones\1
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
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: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown HKLM\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_localmachine_lockdown Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\ Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\ HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\lockdown_zones\ Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\0 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\0 HKCU\software\policies\microsoft\windows\currentversion\internet Opens key: settings\lockdown_zones\0 HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\lockdown_zones\1 HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\lockdown_zones\1 HKCU\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\lockdown_zones\1 HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\lockdown_zones\2 HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\lockdown_zones\2 HKCU\software\policies\microsoft\windows\currentversion\internet Opens key: settings\lockdown_zones\2 HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\lockdown_zones\3 HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\lockdown_zones\3 $\label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\internet}} \\$ Opens key: settings\lockdown_zones\3 HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\lockdown_zones\4 HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\lockdown_zones\4 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\4 Opens kev: HKCU\software\classes\protocols\name-space handler\c\ Opens key: HKCR\protocols\name-space handler\c Opens key: HKCU\software\classes\protocols\handler\c Opens key: HKCR\protocols\handler\c Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000 Opens kev: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000 Opens kev: 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\microsoft\internet explorer\main\featurecontrol\feature_restrict_res_to_lmz Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_res_to_lmz Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_load_shdoclc_resources HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature load shdoclc resources 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 feeds Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature feeds HKCU\software\classes\protocols\filter\text/html Opens kev: Opens key: HKCR\protocols\filter\text/html Opens key: HKCU\software\microsoft\internet

 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-

HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature safe bindtoobject

explorer\main\featurecontrol\feature_safe_bindtoobject

00aa00686f13}\treatas

Opens key:

Opens key: $\label{eq:hkcr} \mbox{HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\} \mbox{\ treatas}$

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

00aa00686f13}\inprocserver32

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

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

00aa00686f13}\inprocserverx86

 $HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserverx86$ Opens key:

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

00aa00686f13}\localserver32

HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\localserver32 Opens key:

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

00aa00686f13}\inprochandler32

 $HKCR \verb|\clsid|{25336920-03f9-11cf-8fd0-00aa00686f13} \verb|\inprochandler32| \\$ Opens key:

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

00aa00686f13}\inprochandlerx86

 $HKCR \c1sid \end{25336920-03f9-11cf-8fd0-00aa00686f13} \label{eq:hkcr} in prochandler x 86 \end{25336920-03f9-11cf-8fd0-00aa00686f13} \end{25336920-036920$ Opens key:

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

00aa00686f13}\localserver

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

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 kev: 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

HKLM\software\microsoft\internet explorer\security\floppy access Opens kev: Opens key: HKCU\software\microsoft\internet explorer\security\adv addrbar spoof

detection

HKLM\software\microsoft\internet explorer\security\adv addrbar spoof Opens key:

detection

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

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

Opens key: HKCR\protocols\handler\about

HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b} Opens key:

Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b} Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas

Opens key:

HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\inprocserver32

Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32

Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\inprocserverx86

Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86 HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-Opens kev:

00aa00bdce0b}\localserver32

HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver32 Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-Opens key:

00aa00bdce0b}\inprochandler32

 $HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\ \ in prochandler 32$ Opens key: Opens kev: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\inprochandlerx86

HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86 Opens key:

Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\localserver

Opens key: $HKCR \clsid \ \{3050f406-98b5-11cf-bb82-00aa00bdce0b\} \localserver$

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

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

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 HKLM\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature weboc document zoom

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

00aa00686f13}\progid

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

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\policies\microsoft\internet explorer HKCU\software\microsoft\internet explorer\international Opens kev:

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\currentcontrol\nls\codepage

Opens key: HKCU\software\microsoft\internet explorer\international\scripts\3
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\mlang.dll

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

Opens key: ${\tt HKLM \setminus software \setminus microsoft \setminus internet \ explorer \setminus vector}$

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

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\rasman.dll

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

options\rtutils.dll

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

options\winmm.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\drivers32 Opens key: HKLM\system\currentcontrol\set\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\currentcontrol\session manager\environment

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

1757981266-507921405-1957994488-1003

Opens key: HKCU\environment

Opens key: HKCU\volatile environment

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

options\sensapi.dll

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_isolate_named_windows Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_isolate_named_windows 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: HKCU\software\microsoft\windows\currentversion\internet settings\url

history

Opens key: HKCU\software\microsoft\internet

 $\begin{tabular}{ll} explorer $$ explorer \rightarrow $$ explorer \Rightarrow$

explorer\main\featurecontrol\feature_codepage_inherit

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

Opens key: HKCR\protocols\name-space handler\http

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

agent

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

agent

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

settings\5.0\user agent

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

settings\5.0\user agent

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

agent\ua tokens

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

agent\pre platform

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

settings\5.0\user agent\pre platform

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

settings\5.0\user agent\pre platform

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

agent\post platform

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

settings\5.0\user agent\post platform

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

settings\5.0\user agent\post platform

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_maxconnectionsperserver Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_maxconnectionsperserver Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_maxconnectionsper1_Oserver

Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_maxconnectionsper1_Oserver

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

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

filters\rpa

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

filters\rpa
Opens key: HKCU\software\microsoft\internet
evalorer\main\featurecontrol\feature include port in san

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

options\mswsock.dll

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

 $Opens~key: \\ HKCU \setminus software \setminus classes \setminus clsid \setminus \{e569bde7-a8dc-47f3-893f-fd2b31b3eefd\}$

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

fd2b31b3eefd}\treatas

fd2b31b3eefd}\inprocserver32

Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\hnetcfg.dll

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

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

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

Opens key: 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

fd2b31b3eefd}\inprochandler32

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

fd2b31b3eefd}\inprochandlerx86

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

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

fd2b31b3eefd}\localserver

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

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

options\wshtcpip.dll

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: HKLM\software\policies\microsoft\internet explorer\restrictions
Opens key: HKCU\software\policies\microsoft\internet explorer\restrictions
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-

 $\verb|f4ceaaf59cfc| \verb|\inprochandler32| \\$

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

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

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\\3ce74de4-53d3-4d74-8b83-8d74-8b83-8d74-8b83-8d74-8d

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}\) in prochandler 32$

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

HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandlerx86 Opens key:

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

869523e2d6c7}\localserver

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

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

Opens key:

c9633f71be64}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}

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

77e8f3d1aa80}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}

HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-Opens key:

e988c088ec82}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}

Opens key: $HKLM \setminus software \setminus microsoft \setminus tip \setminus \{dcbd6fa8-032f-11d3-b5b1-143$

00c04fc324a1}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}

 $HKLM \setminus software \setminus microsoft \setminus tip \setminus \{f89e9e58-bd2f-4008-9ac2-bd2$ Opens key:

Of816c09f4ee}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091} HKCU\software\microsoft\ctf\langbaraddin\ Opens key: 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}

 $HKLM \setminus software \setminus microsoft \setminus tip \setminus \{78cb5b0e-26ed-4fcc-854c-4fc$ Opens key:

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

Opens key: HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddde988c088ec82}\category\{534c48c1-0607-4098-a521-4fc899c73e90}

Opens key: HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-

00c04fc324a1}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}

 $HKLM \setminus software \setminus microsoft \setminus tip \setminus \{f89e9e58-bd2f-4008-9ac2-bd2$ Opens key:

Of816c09f4ee}\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}

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

c9633f71be64}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}

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

77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}

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

c9633f71be64}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}

 $HKLM \setminus software \setminus microsoft \setminus ctf \setminus tip \setminus \{78cb5b0e-26ed-4fcc-854c-4fcc-85$ Opens key:

 $77e8f3d1aa80\} \\ category \\ item \\ \{c6debc0a-f2b2-4f17-930e-ca9faff4cd04\} \\$

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

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

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

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

Opens key: HKLM\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 kev: 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\iphlpapi.dll

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

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

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

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

options\msv1_0.dll

 $\label{lem:hklm} \mbox{HKLM} \mbox{$\mbox{hicrosoft}\windows nt} \mbox{$\mbox{currentversion}$\age file execution}$ Opens key: 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\system\currentcontrolset\services\tcpip\parameters Opens kev:

c7d49d7cecdc}

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

Opens kev: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong

cryptographic provider

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

options\rsaenh.dll

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

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

HKLM\software\microsoft\cryptography\offload

Opens key: HKCU\software\microsoft\internet explorer\searchproviders\ Opens key: HKCU\software\microsoft\internet explorer\ietld\lowmic HKCU\software\microsoft\windows\currentversion\internet Opens kev:

settings\p3p\history\joymax.com

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

Opens key: HKCR\mime\database\content type\text/html; charset=utf-8 HKCU\software\classes\mime\database\content type\text/html Opens key:

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

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

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

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

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

javascript

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561

HKLM\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature cross domain redirect mitigation

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation

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

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

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

00aa00bbbb58}\localserver32

Opens key: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\localserver32 HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-Opens key:

00aa00bbbb58}\inprochandler32

Opens key: $HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprochandler32$

Opens key:

00aa00bbbb58}\inprochandlerx86

Opens key: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprochandlerx86

HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-Opens key: 00aa00bbbb58}\localserver

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

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

options\jscript.dll

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

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547 Opens key: HKLM\system\currentcontrolset\control\nls\locale

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\83497c45d30bcb551f5f55f3f63b6fa1.exe

Opens key: HKCR\appid\83497c45d30bcb551f5f55f3f63b6fa1.exe HKLM\system\currentcontrolset\control\lsa Opens key:

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_use_windowedselectcontrol HKLM\software\microsoft\internet explorer\main\featurecontrol\feature use windowedselectcontrol

 $\label{local-bbs2-00aa00bdce0b} HKCU \setminus software \setminus classes \setminus clsid \setminus \{3050f391-98b5-11cf-bb82-00aa00bdce0b\}$ Opens key:

Opens key: HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b} HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-Opens key:

00aa00bdce0b}\treatas

HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\treatas Opens kev: HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-Opens key:

00aa00bdce0b}\inprocserver32

Opens key: $HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\tinprocserver32$

HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-Opens kev:

00aa00bdce0b}\inprocserverx86

HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86 Opens key:

Opens key: HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-

00aa00bdce0b}\localserver32

HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\localserver32 Opens key:

Opens kev: HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-

00aa00bdce0b}\inprochandler32

 $HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\tinprochandler32$ Opens key:

HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-Opens key:

00aa00bdce0b}\inprochandlerx86

 $HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\ \ in prochandler x 86$ Opens key:

Opens kev: HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-

00aa00bdce0b}\localserver

Opens key: $HKCR \clsid \ \{3050f391-98b5-11cf-bb82-00aa00bdce0b\} \localserver$

HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-Opens key:

00aa00bdce0b}\progid

HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\progid Opens key:

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_xmlhttp

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_xmlhttp

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

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_about_protocol_ie7 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_about_protocol_ie7

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

options\uxtheme.dll

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

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

options\xpsp2res.dll

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

explorer\main\featurecontrol\feature_block_lmz_img

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

HKCR\mime\database\content type\image/jpeg Opens kev:

 $\label{lem:hklm} \verb+Kklm \+ software \+ policies \+ microsoft \+ internet explorer \+ services$ Opens key:

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

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

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

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

explorer\infodelivery\restrictions Opens key:

HKCU\software\policies\microsoft\internet explorer\infodelivery\restrictions

Opens key:

HKLM\software\policies\microsoft\internet explorer\suggested sites

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

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

Oueries value:

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

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

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

nt\currentversion\compatibility32[83497c45d30bcb551f5f55f3f63b6fa1]

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

compatibility[83497c45d30bcb551f5f55f3f63b6fa1]

HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls] Oueries value: Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled] Oueries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]

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

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

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

manager[criticalsectiontimeout]

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

Queries value: HKCR\interface[interfacehelperdisableall]

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

00000000046}[interfacehelperdisableall]

. HKCR\interface\{00020400-0000-0000-c000-Oueries value:

00000000046}[interfacehelperdisableallforole32]

Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[norun] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nodrives] HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetconnectdisconnect] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[norecentdocshistory] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[noclose] Queries value: HKLM\software\microsoft\ctf\systemshared[cuas] Oueries value: HKCU\keyboard layout\toggle[language hotkey] HKCU\keyboard layout\toggle[hotkey] Oueries value: Oueries value: HKCU\keyboard layout\toggle[layout hotkey] Queries value: HKLM\software\microsoft\ctf[enableanchorcontext] HKLM\software\microsoft\windows nt\currentversion\imm[ime file] Oueries value: Queries value: HKCU\software\microsoft\ctf[disable thread input manager] Oueries value: HKLM\software\microsoft\com3[com+enabled] Oueries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess] Queries value: ${\tt HKLM \setminus software \setminus microsoft \setminus ole[minimumfreemempercentage to create object]}$ Queries value: HKLM\software\microsoft\com3[regdbversion] HKCR\clsid\{8856f961-340a-11d0-a96b-Oueries value: 00c04fd705a2}\inprocserver32[inprocserver32] HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32[] Queries value: $HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2\}[appid]$ Queries value: Queries value: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32[threadingmodel] HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe[] Oueries value: Queries value: HKLM\software\microsoft\internet explorer\setup[iexplorelastmodifiedlow] HKLM\software\microsoft\internet Oueries value: explorer\setup[iexplorelastmodifiedhigh] Queries value: HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45ab78-1084642581fb] Oueries value: 0000-0000000000000 Queries value: HKLM\system\currentcontrolset\control\session manager[safeprocesssearchmode] 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[] Oueries value: Queries value: HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32[] Oueries value: $HKCR \verb|\interface|{93f2f68c-1d1b-11d3-a30e-00c04f79abd1} \verb|\proxystubclsid32[]|$ Queries value: HKLM\software\microsoft\rpc[maxrpcsize] Oueries value: Queries value: ${\tt HKLM \ } system \verb| current control \verb| set \verb| computer name \verb| active computer name \verb| [computer name]|$ Queries value: $\label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet$ settings[disableimprovedzonecheck] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[83497c45d30bcb551f5f55f3f63b6fa1.exe] Oueries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[*] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[createuricachesize] Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[createuricachesize] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[enablepunycode] HKLM\software\microsoft\windows\currentversion\internet Queries value: settings[enablepunycode] HKCU\software\microsoft\internet explorer\main[frametabwindow] Oueries value: HKLM\software\microsoft\internet explorer\main[frametabwindow] Queries value: Queries value: HKCU\software\microsoft\internet explorer\main[framemerging] HKLM\software\microsoft\internet explorer\main[framemerging] Oueries value: HKCU\software\microsoft\internet explorer\main[sessionmerging] Oueries value: HKLM\software\microsoft\internet explorer\main[sessionmerging] Queries value: Oueries value: HKCU\software\microsoft\internet explorer\main[admintabprocs] Queries value: HKLM\software\microsoft\internet explorer\main[admintabprocs] HKLM\software\policies\microsoft\internet explorer\main[tabprocgrowth] Oueries value: Queries value: HKCU\software\microsoft\internet explorer\main[tabprocgrowth] HKLM\software\microsoft\internet explorer\main[tabprocgrowth] Oueries value: Oueries value: HKLM\software\microsoft\internet explorer\main[navigationdelay] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nonethood] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]

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

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

HKCU\software\microsoft\windows\currentversion\internet

Queries value:

```
settings\5.0\cache\history[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\history[cachelimit]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacherepair]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\extensible cache\domstore[cachepath]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
 Queries value:
settings\5.0\cache\extensible cache\domstore[cacheoptions]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\feedplat[cacherepair]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\feedplat[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cacherepair]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cachepath]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cachelimit]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\ietld[cacherepair]
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\ietld[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\ietld[cachelimit]
                            \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{$microsoft$} \windows \current version \end{tabular} internet \\ \end{tabular}
 Queries value:
settings\5.0\cache\extensible cache\ietld[cacheoptions]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
                            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]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\privacie:[cacherepair]
 Oueries 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]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\privacie:[cachelimit]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disableworkerthreadhibernation]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[socketreceivebufferlength]
```

```
Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsperserver]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsper1_0server]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsper1_0server]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperproxy]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[serverinfotimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connecttimeout]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connecttimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connectretries]
                            HKI M\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connectretries]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendtimeout]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendtimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[receivetimeout]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[receivetimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablentlmpreauth]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[scavengecachelowerbound]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
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]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelimit]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
                            HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[83497c45d30bcb551f5f55f3f63b6fa1.exe]
 Oueries value:
                            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature disable unicode handle closing callback[*1
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[perusercookies]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[disablent4rascheck]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dialupuselansettings]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dialupuselansettings]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypassftptimecheck]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[releasesocketduringauth]
 Queries value:
                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[releasesocketduring401auth]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[releasesocketduring401auth]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[wpadsearchalldomains]
 Queries value:
                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[disablelegacypreauthasserver]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablelegacypreauthasserver]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[bypasshttpnocachecheck]
```

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

Queries value:

```
settings[bypasshttpnocachecheck]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasssslnocachecheck]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
 Queries value:
                         \label{lem:hklm} \verb+Kklm \+ software \+ microsoft \+ windows \+ current version \+ internet
settings[enablehttptrace]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[nocheckautodialoverride]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
 Queries value:
                         \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[dontusednsloadbalancing]
 Oueries 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]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[headerexclusionlistforcache]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dnscacheenabled]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
                         \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings[dnscachetimeout]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonpost]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnalwaysonpost]
                         \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings[warnonzonecrossing]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonbadcertsending]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonbadcertrecving]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
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\svstem\currentcontrolset\services\winsock2\parameters\protocol catalog9[next catalog entry id]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
 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]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000004[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
 Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000001[displaystring])
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog S \setminus catalog\_entries \setminus 000000000001[providerid]
```

Oueries value:

Oueries value:

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

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

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

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

Queries value:

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

Queries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 0000000000002 \ [displaystring] \ Queries \ value:$

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 00000000000002 [providerid] \\ Queries \ value:$

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

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

Oueries value:

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

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

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000003[supportednamespace]
Oueries value:

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

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

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

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]
Oueries value:

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

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

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

settings[badproxyexpirestime]

Queries value:

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

Queries value: HKCR\protocols\handler\res[clsid]
Queries value: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-

00aa00bdce0b}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]

Queries value: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}[appid]

Queries value: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-

00aa00bdce0b}\inprocserver32[threadingmodel]

Queries value: HKLM\software\microsoft\internet

 $explorer \verb|\main| featurecontrol| feature_legacy_dispparams [83497c45d30bcb551f5f55f3f63b6fa1.exe]|$

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

explorer\main\featurecontrol\feature_object_caching[83497c45d30bcb551f5f55f3f63b6fa1.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[83497c45d30bcb551f5f55f3f63b6fa1.exe]

Queries value: HKCU\software\microsoft\internet explorer\domstorage[totallimit]
Queries value: HKCU\software\microsoft\internet explorer\domstorage[domainlimit]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\ratings[key]

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

settings[urlencoding]

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]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\1[flags]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[flags]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[flags]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\4[flags]
                          HKCU\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[83497c45d30bcb551f5f55f3f63b6fa1.exe]
 Queries value:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
 Oueries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[83497c45d30bcb551f5f55f3f63b6fa1.exe]
                          HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[specialfolderscachesize]
                          HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[specialfolderscachesize]
                          HKCU\software\microsoft\internet explorer[no3dborder]
 Queries value:
                          HKLM\software\microsoft\internet explorer[no3dborder]
 Oueries value:
                          HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_mime_handling[83497c45d30bcb551f5f55f3f63b6fa1.exe]
 Oueries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[*]
                          HKLM\software\microsoft\ole[maximumallowedallocationsize]
 Oueries value:
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing[83497c45d30bcb551f5f55f3f63b6fa1.exe]
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing[*]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[istextplainhonored]
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_feeds[83497c45d30bcb551f5f55f3f63b6fa1.exe]
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_feeds[*]
                          \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{$microsoft$} \windows \current version \end{tabular} internet \\ \end{tabular}
 Queries value:
settings[proxvenable]
                          HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_safe_bindtoobject[83497c45d30bcb551f5f55f3f63b6fa1.exe]
                          HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_safe_bindtoobject[*]
                          HKCR\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32[inprocserver32]
                          HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[]
 Queries value:
                          HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[appid]
 Oueries value:
                          HKCR\clsid\{25336920-03f9-11cf-8fd0-
 Oueries value:
00aa00686f13}\inprocserver32[threadingmodel]
                          {\tt HKCU \backslash software \backslash microsoft \backslash windows}
 Queries value:
nt\currentversion\windows[dragscrollinset]
 Queries value:
                          HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrolldelay]
                          HKCU\software\microsoft\windows
 Oueries value:
nt\currentversion\windows[dragscrollinterval]
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[83497c45d30bcb551f5f55f3f63b6fa1.exe]
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[*]
                          HKCR\protocols\handler\about[clsid]
 Oueries value:
                          HKCR\clsid\{3050f406-98b5-11cf-bb82-
 Queries value:
00aa00bdce0b}\inprocserver32[inprocserver32]
 Queries value:
                          HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
                          HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}[appid]
 Oueries value:
 Queries value:
                          HKCR\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2106]
                          HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\3[2106]
 Queries value:
                          HKCU\software\microsoft\internet explorer\zoom[zoomdisabled]
 Oueries value:
                          HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[]
 Queries value:
                          HKLM\software\policies\microsoft\internet explorer[smartdithering]
 Oueries value:
                          HKCU\software\microsoft\internet explorer[smartdithering]
 Oueries value:
                          HKCU\software\microsoft\internet explorer[rtfconverterflags]
 Oueries value:
                          HKLM\software\policies\microsoft\internet explorer\main[usecleartype]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[usecleartype]
 Oueries value:
                          HKLM\software\policies\microsoft\internet
```

explorer\main[page_transitions]

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

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

explorer\main[use_dlgbox_colors]

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

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

images]

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

videos1

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

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

explorer\main[play_background_sounds]

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

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

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

explorer\main[print_background]

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

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

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

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

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

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

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

Oueries value: HKCU\software\microsoft\internet

explorer\international[default_codepage]

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

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

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

face1

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

programmatic cut_copy_paste]

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

Oueries 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]

HKCU\software\microsoft\internet Oueries value:

explorer\international\scripts\3[iefixedfontname]

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

Oueries 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[83497c45d30bcb551f5f55f3f63b6fa1.exe]

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

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

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[83497c45d30bcb551f5f55f3f63b6fa1.exe]

HKLM\software\microsoft\internet Oueries value:

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]

HKI M\software\microsoft\windows\currentversion\internet Oueries value:

settings\zones\0[2106]

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

settings[cointernetcombineiuricachesize]

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

settings[cointernetcombineiuricachesize]

HKLM\software\microsoft\windows nt\currentversion\drivers32[wave] Oueries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2] HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3] Oueries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4] Oueries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9] Queries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2] Oueries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3] Oueries value: $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [aux 4]$ Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]

HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer31 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4] HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7] HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9] Oueries value:

Oueries value:

Queries value:

HKLM\software\microsoft\windows\currentversion\telephony[tapi32maxnumrequestretries]

Queries value:

Queries value: HKLM\software\microsoft\tracing[enableconsoletracing] Oueries value: HKLM\software\microsoft\tracing\rasapi32[enablefiletracing] Queries value: HKLM\software\microsoft\tracing\rasapi32[filetracingmask] Oueries value: HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing] Oueries value: HKLM\software\microsoft\tracing\rasapi32[consoletracingmask] Queries value: HKLM\software\microsoft\tracing\rasapi32[maxfilesize] Queries value: HKLM\software\microsoft\tracing\rasapi32[filedirectory]

 $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} windows \end{tabular} current version \end{tabular} explorer \end{tabular} user shell$ Oueries value:

folders[common appdata]

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\winlogon[userenvdebuglevel]

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\winlogon[chkaccdebuglevel]

HKLM\svstem\currentcontrolset\control\productoptions[producttype] Oueries value: Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[personal] HKCU\software\microsoft\windows\currentversion\explorer\user shell Oueries value: folders[local settings] Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsopdebuglevel] Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging] Oueries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[profilesdirectory] Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[allusersprofile] Oueries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[defaultuserprofile] Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir] Oueries 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] HKCU\software\microsoft\windows Oueries value: 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] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[proxyserver] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[proxyoverride] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[autoconfigurl] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\connections[savedlegacysettings] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\connections[defaultconnectionsettings] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zonemap[autodetect] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\url history[daystokeep] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\3[2700] HKLM\software\microsoft\windows\currentversion\internet Queries value: settings\zones\3[2700] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\user agent[] HKLM\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\user agent[] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\user agent[compatible] Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent[compatible] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\user agent[version] Oueries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent[version] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[user agent] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\user agent[platform] Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent[platform] Oueries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_maxconnectionsperserver[83497c45d30bcb551f5f55f3f63b6fa1.exe] HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_maxconnectionsperserver[*] HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_maxconnectionsper1_0server[83497c45d30bcb551f5f55f3f63b6fa1.exe] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_maxconnectionsper1_0server[*] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[securityidiuricachesize] Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[securitvidiuricachesize] Queries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel] Oueries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports] HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping] Oueries value: Oueries value: HKCR\clsid\{e569bde7-a8dc-47f3-893ffd2b31b3eefd}\inprocserver32[inprocserver32] Oueries value: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32[] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength] Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
 Queries value:

```
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
                                     HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}[appid]
  Oueries value:
  Oueries value:
                                     HKCR\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32[threadingmodel]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[warnonintranet]
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion\internet
settings[warnonintranet]
                                     HKCR\clsid\{50d5107a-d278-4871-8989-
  Queries value:
f4ceaaf59cfc}\inprocserver32[inprocserver32]
                                     HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32[]
  Oueries value:
  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]
                                     HKCR\clsid\{3ce74de4-53d3-4d74-8b83-
  Oueries value:
431b3828ba53}\inprocserver32[inprocserver32]
  Queries value:
                                     HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32[]
                                     HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}[appid]
  Oueries value:
  Queries value:
                                     HKCR\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprocserver32[threadingmodel]
                                    HKCR\clsid\{a4b544a1-438d-4b41-9325-
  Oueries value:
869523e2d6c7}\inprocserver32[inprocserver32]
  Queries value:
                                     HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserver32[]
                                     HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}[appid]
  Queries value:
  Queries value:
                                     HKCR\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprocserver32[threadingmodel]
                                     HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
  Oueries value:
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}[description]
  Queries value:
                                     HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[description]
                                     HKLM \setminus software \setminus icrosoft \setminus tip \setminus \{78cb5b0e-26ed-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc
  Queries value:
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}[description]
                                     HKCU\software\microsoft\internet explorer\recovery[autorecover]
  Oueries value:
  Queries value:
                                     \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\zones\0[2000]
                                     HKLM\software\microsoft\internet explorer\feed discovery[sound]
  Oueries value:
  Queries value:
                                     HKCU\software\microsoft\ftp[use web based ftp]
  Queries value:
                                     HKLM\software\microsoft\rpc\securityservice[10]
  Oueries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
                                     HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
  Oueries value:
  Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]
                                     {\tt HKLM \ } system \verb|\ current control \verb|\ lsa \ | sspicache \verb|\ msapsspc.dll[rpcid]|
  Queries value:
  Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[version]
                                     HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]
  Oueries value:
  Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]
                                     HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]
  Queries value:
  Oueries value:
                                     HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities]
                                     HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid]
  Oueries value:
                                     HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version]
  Oueries value:
  Queries value:
                                     HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize]
                                     HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name]
  Queries value:
                                     HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment]
  Oueries value:
  Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities]
  Queries value:
                                     HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid]
                                     Queries value:
  Queries value:
                                     HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type]
  Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize]
                                     HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
  Oueries value:
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1a10]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [used omain name devolution]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
 Oueries 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]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
 Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
                       HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
 Queries value:
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
                       HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
 Queries value:
 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:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [disable reverse address registrations]
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [registration ttl]
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
 Oueries value:
HKLM \setminus system \setminus current controls et \setminus services \setminus dns cache \setminus parameters [update top level domain zones]
                       HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
 Queries value:
 Queries value:
                       HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
 Oueries value:
                       Queries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
 Queries value:
                       HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
 Oueries value:
```

```
c7d49d7cecdc}[enabledhcp]
      Oueries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-a
 c7d49d7cecdc}[leaseobtainedtime]
      Oueries value:
c7d49d7cecdc}[leaseterminatestime]
      Oueries value:
c7d49d7cecdc}[dhcpserver]
                                                                                       HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
      Oueries value:
      Queries value:
                                                                                       HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
      Oueries value:
c7d49d7cecdc}[queryadaptername]
c7d49d7cecdc}[disableadapterdomainname]
      Oueries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-4404, and the services \ tcpip \ parameters \ terrange \ terr
c7d49d7cecdc}[registrationenabled]
      Oueries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-a
 c7d49d7cecdc}[registeradaptername]
      Queries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-4404, and the services \ tcpip \ parameters \ terrange \ terr
c7d49d7cecdc}[registrationmaxaddresscount]
      Queries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-a
 c7d49d7cecdc}[maxnumberofaddressestoregister]
      Oueries value:
c7d49d7cecdc}[domain]
      Queries value:
c7d49d7cecdc}[dhcpdomain]
      Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[ipautoconfigurationenabled]
      Queries value:
c7d49d7cecdc}[addresstype]
      Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[nameserver]
      Queries value:
c7d49d7cecdc}[dhcpnameserver]
                                                                                       HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
      Oueries value:
      Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
                                                                                       HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
      Oueries value:
 cryptographic provider[type]
                                                                                       HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
      Queries value:
cryptographic provider[image path]
                                                                                       HKLM\software\microsoft\cryptography[machineguid]
      Queries value:
                                                                                        HKCU\software\microsoft\internet
      Oueries value:
explorer\ietld\lowmic[ietlddllversionlow]
                                                                                       HKCU\software\microsoft\internet
      Queries value:
 explorer\ietld\lowmic[ietlddllversionhigh]
      Queries value:
                                                                                       HKCU\software\microsoft\windows\currentversion\internet
 settings\zones\3[{a8a88c49-5eb2-4990-a1a2-0876022c854f}]
                                                                                       HKCU\software\microsoft\windows\currentversion\internet
      Queries value:
settings[privacyadvanced]
                                                                                       HKCR\mime\database\content type\text/html[extension]
      Queries value:
                                                                                        HKLM\software\microsoft\internet
      Oueries value:
explorer\main\featurecontrol\feature_subdownload_lockdown[83497c45d30bcb551f5f55f3f63b6fa1.exe]
      Queries value:
                                                                                       HKLM\software\microsoft\internet
 explorer\main\featurecontrol\feature_subdownload_lockdown[*]
                                                                                       HKCU\software\microsoft\windows\currentversion\internet
      Oueries value:
 settings[privdiscuishown]
                                                                                       HKCU\software\microsoft\windows\currentversion\internet
      Oueries value:
 settings\zones\3[1400]
```

HKCR\clsid\{f414c260-6ac0-11cf-b6d1-

HKCR\clsid\{f414c260-6ac0-11cf-b6d1-

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

 $HKCR \clsid \f414c260-6ac0-11cf-b6d1-00aa00bbbb58 \clsid \align{transfer} [appid]$

HKCU\software\microsoft\windows\currentversion\internet

HKLM\system\currentcontrolset\control\nls\locale[00000409]

HKLM\system\currentcontrolset\control\nls\language groups[1]

Queries value:

Oueries value:

Queries value:

Oueries value:

Oueries value:

Queries value: Queries value:

settings\zones\3[1201]

00aa00bbbb58}\inprocserver32[inprocserver32]

00aa00bbbb58}\inprocserver32[threadingmodel]

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

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

Oueries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_use_windowedselectcontrol[83497c45d30bcb551f5f55f3f63b6fa1.exe]

Oueries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_use_windowedselectcontrol[*]

HKCU\software\microsoft\windows script\settings[jitdebug] Oueries value:

HKCR\clsid\{3050f391-98b5-11cf-bb82-Oueries value:

00aa00bdce0b}\inprocserver32[inprocserver32]

HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[] Queries value:

Oueries value: HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}[appid] Queries value: HKLM\software\microsoft\internet explorer\abouturls[blank]

Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[compositing]

HKCU\control panel\desktop[lamebuttontext] Oueries value:

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

folders[local appdata]

HKLM\software\microsoft\internet explorer\main[maxrenderline] Oueries value:

Queries value: HKCR\mime\database\content type\image/jpeg[extension]

Queries value: HKCU\software\microsoft\internet

explorer\services[selectionactivitybuttondisable]

Queries value: HKCU\software\microsoft\internet explorer\suggested sites[enabled]

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

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

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

settings\zonemap[proxybypass]

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

settings\zonemap[intranetname]

Value changes:

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

settings\zonemap[uncasintranet]

 $\label{lem:hkcu} \mbox{HKCU\software\mbox{\sc urrentversion\sc internet}} \\$ Value changes:

settings\zonemap[autodetect]

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

folders[common appdata]

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

folders[appdata]

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

settings[proxyenable]

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

settings\connections[savedlegacysettings]

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

folders[local appdata]