Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 619, Task ID: 2422

Task ID: 2422

Risk Level:

Date Processed: 2016-02-22 05:28:19 (UTC)

61.64 seconds Processing Time: IntelliVM Virtual Environment:

Execution Arguments:

c:\windows\temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe"

619 Sample ID: Type: basic Owner:

81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22 Label:

Date Added: 2016-02-22 05:26:49 (UTC)

File Type: PE32:win32:gui File Size: 286720 bytes

MD5: 6f2159e72e7ab7b02e18211ecbed7dd3

SHA256: 81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22

Description:

Pattern Matching Results

5 Creates process in suspicious location

1 YARA score 1

Modifies registry autorun entries

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

6 Dumps and runs batch script

5 Adds autostart object

4 Terminates process under Windows subfolder

Static Events

YARA rule hit: 0LE2 YARA rule hit: Nonexecutable

Process/Thread Events

Creates process:

C:\WINDOWS\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe ["c:\windows\temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe"]

Creates process: C:\Documents and Settings\All Users\WinJab\winjab.exe ["C:\Documents and

Settings\All Users\WinJab\winjab.exe"]

Creates process: C:\WINDOWS\system32\cmd.exe [cmd /c C:\DOCUME~1\ALLUSE~1\1.bat] Terminates process:

C:\WINDOWS\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe

Terminates process: C:\WINDOWS\system32\cmd.exe

Named Object Events

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

1957994488-1003

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

1957994488-1003

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

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

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

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!temporarv internet files!content.ie5!

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

settings!history!history.ie5!

\BaseNamedObjects\WininetConnectionMutex Creates mutex: Creates semaphore: \BaseNamedObjects\C:?WINDOWS?TEMP? 81F686A320DBEC38A90D64C98861F8DDAC8BFDAA7F1AD04A8A33961283E00A22.EXE

Creates semaphore: \BaseNamedObjects\OleDfRoot000021FDE

\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1} Creates semaphore: \BaseNamedObjects\C:?DOCUMENTS AND SETTINGS?ALL USERS?WINJAB?WINJAB.EXE Creates semaphore:

\BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D} Creates semaphore:

Creates semaphore: \BaseNamedObjects\OleDfRoot00002503D

File System Events

Creates: C:\Documents and Settings\Admin\Local Settings\Temp\~DF1FE1.tmp

Creates C:\Documents and Settings\All Users\WinJab

Creates C:\Documents and Settings\All Users\WinJab\winjab.exe Creates: C:\WINDOWS\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22

C:\Documents and Settings\All Users\1.bat Creates:

 ${\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\~DF5040.tmp}$ Creates: C:\WINDOWS\Prefetch\81F686A320DBEC38A90D64C98861F-0071ABEB.pf Opens:

Opens: C:\Documents and Settings\Admin C:\WINDOWS\system32\msvbvm60.dll Opens: C:\WINDOWS\system32\imm32.dll Opens: C:\WINDOWS\system32\rpcss.dll Opens: C:\WINDOWS\system32\MSCTF.dll Opens:

```
Opens:
                         C:\WINDOWS\system32\sxs.dll
 Opens:
                         C:\WINDOWS\system32\MSCTFIME.IME
 Opens:
                         C:\WINDOWS\system32\winmm.dll
 Opens:
                         C:\WINDOWS\system32\MSIMTF.dll
                         C:\WINDOWS\Fonts\sserife.fon
 Opens:
                         C:\WINDOWS\Fonts\verdanab.ttf
 Opens:
                         C:\WINDOWS\Fonts\lucon.ttf
 Opens:
                         C:\WINDOWS\system32\clbcatq.dll
 Opens:
                         C:\WINDOWS\system32\comres.dll
 Opens:
                         C:\WINDOWS\Registration\R00000000007.clb
 Opens:
 Opens:
                         C:\WINDOWS\system32\ieframe.dll
                         C:\WINDOWS\system32\shell32.dll
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Config
 Opens:
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
 Opens:
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
 Opens:
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comct132.dll
                         C:\WINDOWS\WindowsShell.Manifest
 Opens:
                         C:\WINDOWS\WindowsShell.Config
 Opens:
 Opens:
                         C:\WINDOWS\system32\comctl32.dll
                         C:\WINDOWS\system32\comctl32.dll.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Config
 Opens:
                         C:\Program Files\Internet Explorer\iexplore.exe
 Opens:
                         C:\WINDOWS\system32\ieframe.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\ieframe.dll.123.Config
                         C:\WINDOWS\system32\en-US\ieframe.dll.mui
 Opens:
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Config
                         C:\WINDOWS\Fonts\verdana.ttf
 Opens:
                         C:\WINDOWS\system32\asycfilt.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\winhttp.dll
 Opens:
                         C:\WINDOWS\system32\ws2_32.dll
 Opens:
                         C:\WINDOWS\system32\ws2help.dll
                         C:\WINDOWS\system32\mswsock.dll
 Opens
 Opens:
                         C:\WINDOWS\system32\hnetcfg.dll
 Opens:
                         C:\WINDOWS\system32\wshtcpip.dll
 Opens:
                         C:\WINDOWS\system32\dnsapi.dll
 Opens:
                         C:\WINDOWS\system32\iphlpapi.dll
 Opens:
                         C:\WINDOWS\system32\drivers\etc\hosts
 Opens:
                         C:\WINDOWS\system32\rsaenh.dll
 Opens:
                         C:\WINDOWS\system32\crypt32.dll
 Opens:
                         C:\WINDOWS\system32\rasadhlp.dll
 Opens:
                         C:\WINDOWS\system32\scrrun.dll
 Opens:
                         C:\WINDOWS\Temp
 Opens:
C:\WINDOWS\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe
 Opens:
                         C:\Documents and Settings\All Users\WinJab
 Opens:
                         C:\Documents and Settings\All Users\WinJab\winjab.exe
                         C:\WINDOWS\system32\apphelp.dll
 Opens:
                         C:\WINDOWS\AppPatch\sysmain.sdb
 Opens:
                         C:\WINDOWS\AppPatch\systest.sdb
 Opens:
 Opens:
                         C:\Documents and Settings\All Users
                         C:\Documents and Settings\All Users\WinJab\winjab.exe.Manifest
 Opens:
                         C:\WINDOWS\Prefetch\WINJAB.EXE-25F28A73.pf
 Opens:
 Opens
C:\WINDOWS\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22
                         C:\WINDOWS\Temp\3e0228b0-0f27-47e2-88e1-ce66e0836ba4
 Opens:
 Opens:
                         C:\
                         C:\Documents and Settings
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\1.bat
 Opens:
                         C:\WINDOWS\system32\cmd.exe
 Opens:
                         C:\WINDOWS\system32\cmd.exe.Manifest
 Opens:
                         C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf
 Opens:
                         C:\WINDOWS\system32\WININET.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\WININET.dll.123.Config
 Opens:
                         C:
                         C:\WINDOWS
 Opens:
                         C:\WINDOWS\AppPatch
 Opens
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
 Opens
                         C:\WINDOWS\system32
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens
Files\Content.IE5
                         C:\WINDOWS\system32\wbem
 Opens:
 Opens:
                         C:\WINDOWS\WinSxS
 Opens:
                         C:\WINDOWS\system32\ntdll.dll
 Opens:
                         C:\WINDOWS\system32\kernel32.dll
 Opens:
                         C:\WINDOWS\system32\unicode.nls
 Opens:
                         C:\WINDOWS\system32\locale.nls
 Opens:
                         C:\WINDOWS\system32\sorttbls.nls
 Opens:
                         C:\WINDOWS\system32\msvcrt.dll
 Opens:
                         C:\WINDOWS\system32\user32.dll
 Opens:
                         C:\WINDOWS\system32\gdi32.dll
 Opens:
                         C:\WINDOWS\system32\shimeng.dll
 Opens:
                         C:\WINDOWS\AppPatch\AcGenral.dll
                         C:\WINDOWS\system32\advapi32.dll
 Opens:
                         C:\WINDOWS\system32\rpcrt4.dll
 Opens:
                         C:\WINDOWS\system32\secur32.dll
 Opens:
                         C:\WINDOWS\system32\ole32.dll
 Opens:
                         C:\WINDOWS\system32\oleaut32.dll
 Opens:
                         C:\WINDOWS\system32\msacm32.dll
 Opens:
                         C:\WINDOWS\system32\version.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\shlwapi.dll
                         C:\WINDOWS\system32\userenv.dll
 Opens:
```

```
Opens:
                         C:\WINDOWS\system32\uxtheme.dll
Opens:
                         C:\WINDOWS\system32\ctype.nls
Opens:
                         {\tt C:\WINDOWS\system32\sortkey.nls}
```

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

Opens: C:\WINDOWS\system32\wbem\wmic.exe ${\tt C:\Documents\ and\ Settings\Admin\Cookies}$ Opens: C:\Documents and Settings\Admin\Cookies\index.dat Opens:

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

Settings\History\History.IE5\index.dat

C:\WINDOWS\WINHELP.INI Opens:

Opens: C:\Documents and Settings\Admin\Local Settings\Temp\~DF1FE1.tmp

C:\DOCUME~1\ALLUSE~1\1.bat Opens:

C:\Documents and Settings\All Users\WinJab\winjab.exe Writes to:

C:\Documents and Settings\All Users\1.bat Writes to: Reads from: C:\WINDOWS\Registration\R00000000007.clb Reads from: C:\WINDOWS\system32\drivers\etc\hosts Reads from: C:\WINDOWS\system32\rsaenh.dll Reads from: C:\WINDOWS\system32\scrrun.dll

Reads from:

C:\WINDOWS\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe

Reads from: C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf Reads from: C:\Documents and Settings\All Users\1.bat

Deletes:

C:\WINDOWS\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22

Opens key:

options\msvcrt.dll Opens key:

options\ole32.dll Opens key:

options\oleaut32.dll Opens key:

options\msvbvm60.dll

C:\WINDOWS\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe C:\Documents and Settings\Admin\Local Settings\Temp\~DF1FE1.tmp Deletes:

C:\Documents and Settings\All Users\1.bat

Network Events

DNS query: muzanaczekanie.pl

DNS response: muzanaczekanie.pl ⇒ 188.165.23.155

Connects to: 188.165.23.155:80

Sends data to: 8.8.8.8:53

muzanaczekanie.pl:80 (188.165.23.155) Sends data to:

0.0.0.0:0 Receives data from:

muzanaczekanie.pl:80 (188.165.23.155) Receives data from:

Windows Registry Events	
Creates key:	HKLM\system\currentcontrolset\services\tcpip\parameters
Creates key:	HKCU\software\microsoft\windows\currentversion\run
Creates key:	HKCU\software\vb and vba program settings\clock\sdata
Creates key:	HKCU\software
Creates key:	HKCU\software\vb and vba program settings
Creates key:	HKCU\software\vb and vba program settings\clock
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings
Creates key:	HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders	·
Creates key:	HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Deletes value:	HKCU\software\microsoft\internet
explorer\lowregistry[addtofavoritesinitialselection]	
Deletes value:	HKCU\software\microsoft\internet
explorer\lowregistry[addtofeedsinitialselection]	
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>
options\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe	
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	<pre>HKLM\software\policies\microsoft\windows\safer\codeidentifiers</pre>
Opens key:	<pre>HKCU\software\policies\microsoft\windows\safer\codeidentifiers</pre>
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>
options\gdi32.dll	
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>
options\user32.dll	
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>
options\imm32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntdll.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kernel32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\secur32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll	and the second s

Opens key: HKLM\system\currentcontrolset\control\error message instrument\ Opens key: ${\tt HKLM \ } system \verb| current control \verb| set \verb| control \verb| error message instrument \\$ Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ gre_initialize$ Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32 Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility

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

 $\label{lem:hklmsoftware} \verb+wicrosoft+ windows nt+ current version+ image file execution$

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

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

```
Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\windows
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\winlogon
  Opens key:
                                    HKI M\
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\diagnostics
  Opens key:
                                    HKLM\software\microsoft\ole
  Opens key:
                                    HKCR\interface
                                    HKCR\interface\{00020400-0000-0000-c000-00000000046}
  Opens key:
  Opens key:
                                    HKLM\software\microsoft\oleaut
  Opens key:
                                    HKLM\software\microsoft\oleaut\userera
                                    HKCU\
  Opens kev:
  Opens key:
                                    HKCU\software\policies\microsoft\control panel\desktop
  Opens key:
                                    {\tt HKCU \backslash control\ panel \backslash desktop}
  Opens key:
                                    \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constraint of the constr
options\msctf.dll
  Opens key:
HKLM\software\microsoft\ctf\compatibility\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe
                                    HKLM\software\microsoft\ctf\systemshared\
  Opens kev:
  Opens kev:
                                    HKCU\kevboard lavout\toggle
  Opens key:
                                    HKLM\software\microsoft\ctf\
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\sxs.dll
  Opens key:
                                    HKLM\system\setup
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\imm
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
  Opens key:
                                    HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctfime.ime
  Opens key:
                                    HKCU\software\microsoft\ctf
  Opens key:
                                    HKLM\software\microsoft\ctf\systemshared
  Opens key:
                                    HKLM\system\currentcontrolset\control\nls\codepage
  Opens key:
                                    HKLM\software\microsoft\vba\monitors
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winmm.dll
                                    HKLM\software\microsoft\windows nt\currentversion\drivers32
  Opens key:
  Opens key:
HKLM\software\microsoft\com3
  Opens key:
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comres.dll
  Opens key:
                                    \label{lem:hklmsoftware} \verb+wicrosoft+ windows nt+ current version+ image file execution
options\clbcatq.dll
  Opens key:
                                    HKLM\software\microsoft\com3\debug
  Opens key:
                                    HKCU\software\classes\
  Opens key:
                                    HKLM\software\classes
  Opens key:
                                    HKU\
  Opens key:
                                    HKCR\clsid
  Opens key:
                                    \label{locality} $$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 key:
  Opens kev:
                                    HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32
  Opens key:
                                    HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32
                                    HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
  Opens key:
00c04fd705a2}\inprocserverx86
                                    HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserverx86
  Opens key:
  Opens kev:
                                    HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\localserver32
                                    HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\localserver32
  Opens kev:
  Opens key:
                                    HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandler32
                                    HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler32
  Opens key:
  Opens key:
                                    HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandlerx86
  Opens key:
                                   HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandlerx86
  Opens key:
                                    HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\localserver
  Opens key:
                                    HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\localserver
  Opens key:
                                    \label{lem:hklmsoftware} \verb+wicrosoft+ windows nt+ current version+ image file execution
options\shlwapi.dll
  Opens key:
                                    HKLM\software\microsoft\windows\currentversion\explorer\performance
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shell32.dll
  Opens key:
HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\comctl32.dll
  Opens key:
                                    \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ advanced
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\languagepack
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iertutil.dll
  Opens key:
                                    \label{lem:hklmsoftware} \verb+wicrosoft+ windows nt+ current version+ image file execution
options\ieframe.dll
  Opens key:
                                    HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe
  Opens key:
                                    HKLM\software\microsoft\internet explorer\setup
  Opens key:
                                    HKLM\system\currentcontrolset\control\wmi\security
  Opens key:
                                    HKCU\software\classes\interface\{eab22ac1-30c1-11cf-a7eb-
0000c05bae0b}\typelib
                                    HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib
  Opens key:
```

 $\label{thm:hkcu} HKCU \software \classes \clsid \a4a1a128-768f-41e0-bf75-e4fddd701cba\} \\ HKCR \clsid \a4a1a128-768f-41e0-bf75-e4fddd701cba\}$

HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc-

Opens key: Opens key:

Opens key:

```
00aa00404770}\proxystubclsid32
   Opens key:
                                              HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32
   Opens key
                                              HKCU\software\classes\interface\{79eac9c4-baf9-11ce-8c82-
00aa004ba90b}\proxystubclsid32
   Opens key:
                                              HKCR \verb|\interface|{79eac9c4-baf9-11ce-8c82-00aa004ba90b} \verb|\proxystubclsid32||
   Opens key
                                              HKCU\software\classes\interface\{000214e6-0000-0000-c000-
000000000046}\proxystubclsid32
                                              \label{local-eq:hkcr} \mbox{HKCR} \mbox{ interface} \mbox{\{000214e6-0000-0000-c000-00000000046\}} \mbox{\partial-proxystubclsid32.}
   Opens key:
   Opens kev:
                                              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 key:
                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe\rpcthreadpoolthrottle
   Opens kev:
                                              HKLM\software\policies\microsoft\windows nt\rpc
   Opens kev:
                                              HKLM\system\currentcontrolset\control\computername
                                              HKLM\system\currentcontrolset\control\computername\activecomputername
   Opens kev:
   Opens key:
                                              HKCU\software\classes\clsid\{00021401-0000-0000-c000-00000000046}
                                              HKCR\clsid\{00021401-0000-0000-c000-00000000046}
   Opens key:
                                              HKCU\software\classes\clsid\{00021401-0000-0000-c000-
   Opens key:
000000000046}\treatas
   Opens key:
                                              HKCR\clsid\{00021401-0000-0000-c000-00000000046}\treatas
   Opens key:
                                              HKCU\software\classes\clsid\{00021401-0000-0000-c000-
000000000046}\inprocserver32
                                              HKCR\clsid\{00021401-0000-0000-c000-00000000046}\inprocserver32
   Opens key:
   Opens key
                                              HKCU\software\classes\clsid\{00021401-0000-0000-c000-
00000000046}\inprocserverx86
   Opens key:
                                              HKCR\clsid\{00021401-0000-0000-c000-00000000046}\inprocserverx86
   Opens key:
                                              HKCU\software\classes\clsid\{00021401-0000-0000-c000-
000000000046}\localserver32
   Opens key:
                                              HKCR\clsid\{00021401-0000-0000-c000-00000000046}\localserver32
   Opens key:
                                              HKCU\software\classes\clsid\{00021401-0000-0000-c000-
000000000046}\inprochandler32
                                              HKCR\clsid\{00021401-0000-0000-c000-00000000046}\inprochandler32
   Opens key:
   Opens key:
                                              HKCU\software\classes\clsid\{00021401-0000-0000-c000
00000000046}\inprochandlerx86
                                              HKCR\clsid\{00021401-0000-0000-c000-00000000046}\inprochandlerx86
   Opens key:
   Opens key:
                                              HKCU\software\classes\clsid\{00021401-0000-0000-c000-
000000000046}\localserver
   Opens key:
                                              \label{localserver} \mbox{HKCR\clsid\closed} \mbox{\clsid\closed} \mbox{\clsid\closed} \mbox{\clsid\closed} \mbox{\clsid\clsid\closed} \mbox{\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\
   Opens key:
                                              \label{lem:hklmsoftware} \verb+MKLM+ software+ \verb+microsoft+ windows nt+ current version+ image file execution
options\urlmon.dll
   Opens key:
                                              HKCU\software\classes\protocols\name-space handler\
   Opens key:
                                              HKCR\protocols\name-space handler
   Opens key:
                                              HKCU\software\classes\protocols\name-space handler
   Opens key:
                                              HKCU\software\policies\microsoft\windows\currentversion\internet
settings
   Opens key:
                                              HKLM\software\microsoft\windows\currentversion\internet settings
   Opens key:
                                              HKLM\software\policies\microsoft\windows\currentversion\internet
settings
                                             HKCU\software\microsoft\internet
  Onens key
explorer\main\featurecontrol\feature_protocol_lockdown
                                              HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_protocol_lockdown
  Opens key:
                                              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\
   Opens key:
                                              HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
   Opens kev:
                                              HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
                                              HKLM\software\microsoft\internet explorer\main\featurecontrol
   Opens kev:
                                              HKCU\software\microsoft\internet explorer\main\featurecontrol
   Opens kev:
   Opens key:
                                              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature ignore policies zonemap if esc enabled kb918915
  Opens key:
                                              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
  Opens key:
                                              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:
                                              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:
                                              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
                                              \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \end{tabular} software \end{tabular} policies \end{tabular} irrestor \end{tabular} windows \end{tabular} current version \end{tabular} in terms \end{tabular} and \end{tabular} irrestor \end{tabular} windows \end{tabular} and \end{tabular} irrestor \end{tabular} irrestor \end{tabular} windows \end{tabular} irrestor \end{tabular} windows \end{tabular} irrestor \end{tabular} irrestor \end{tabular} irrestor \end{tabular} windows \end{tabular} irrestor \end{tabular} irrestor \end{tabular} irrestor \end{tabular} windows \end{tabular} w
   Opens key:
settings\zonemap\ranges\
                                              HKCU\software\microsoft\internet
   Opens kev:
explorer\main\featurecontrol\feature_unc_savedfilecheck
                                              HKLM\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_unc_savedfilecheck
   Opens key:
                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\asycfilt.dll
   Opens key:
                                              HKCU\software\policies\microsoft\control
panel\international\calendars\twodigityearmax
   Opens key:
                                              HKCU\control panel\international\calendars\twodigityearmax
   Opens key:
                                              HKCU\software\classes\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}
   Opens key:
                                              HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}
   Opens key
                                              HKCU\software\classes\clsid\{2087c2f4-2cef-4953-a8ab-
66779b670495}\treatas
                                              HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\treatas
   Opens key:
   Opens key:
                                              HKCU\software\classes\clsid\{2087c2f4-2cef-4953-a8ab-
```

 Opens key:
 HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\inprocserverx86

 Opens key:
 HKCU\software\classes\clsid\{2087c2f4-2cef-4953-a8ab

HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\inprocserver32

HKCU\software\classes\clsid\{2087c2f4-2cef-4953-a8ab-

66779b670495}\inprocserver32

66779b670495}\inprocserverx86

Opens kev:

Opens key:

66779b670495}\localserver32 HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\localserver32 Opens key: Opens key: HKCU\software\classes\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\inprochandler32 Opens key: HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\inprochandler32 Opens key: HKCU\software\classes\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\inprochandlerx86 Opens key: HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\inprochandlerx86 Opens kev: HKCU\software\classes\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\localserver HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\localserver Opens key: $\label{lem:hklmsoftware} \verb+MKLM+ software+ \verb+microsoft+ windows nt+ current version+ image file execution$ Opens key: options\winhttp.dll HKLM\software\microsoft\windows\currentversion\internet Opens key: settings\winhttp\tracing HKLM\software\microsoft\windows\currentversion\internet settings\winhttp Opens kev: HKLM\software\microsoft\windows\currentversion\internet Opens kev: settings\connections HKLM\software\microsoft\windows\currentversion\internet Opens key: settings\winhttp\unsafesslapps HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\ws2help.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ws2_32.dll Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9 Opens key: Opens kev: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\00000000010 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\00000004 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000000 Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mswsock.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\hnetcfg.dll Opens key: HKLM\software\microsoft\rpc\securityservice Opens key: HKLM\system\currentcontrolset\services\winsock\parameters Opens key: $\label{lem:hklm} \verb+Kklm \system \current control set \services \tcpip \parameters \winsock \end{tabular}$ Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wshtcpip.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dnsapi.dll Opens 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 key: $\label{lem:hklmsoftware} \verb+microsoft+ windows nt+ current version+ image file execution$ options\iphlpapi.dll Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\ Opens key: $\label{lem:hklm} \verb+Kklm \system \current control set \services \net bt \parameters \net faces$ Opens key: ${\tt HKLM \setminus system \setminus current control set \setminus services \setminus parameters}$ Opens key:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc} HKLM\software\policies\microsoft\system\dnsclient Opens key: Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ cryptography\+ defaults\+ provider\+ microsoft\+ strong$ 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 key:
                                                                  HKLM\software\microsoft\cryptography\offload
    Opens key:
                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasadhlp.dll
    Opens key:
                                                                  HKCU\software\classes\scripting.filesystemobject
    Opens key:
                                                                  HKCR\scripting.filesystemobject
                                                                  HKCU\software\classes\scripting.filesystemobject\clsid
    Opens key:
    Opens key:
                                                                  {\tt HKCR \backslash scripting.filesystemobject \backslash clsid}
                                                                  HKCU \setminus software \setminus classes \setminus clsid \setminus \{0d43fe01-f093-11cf-8940-00a0c9054228\}
    Opens key:
                                                                  HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}
    Opens kev:
                                                                  HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-
    Opens kev:
00a0c9054228}\treatas
                                                                  HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\treatas
    Opens key:
    Opens key:
                                                                  00a0c9054228}\inprocserver32
                                                                  HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\inprocserver32
    Opens kev:
                                                                  HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-
    Opens kev:
00a0c9054228}\inprocserverx86
                                                                 HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\inprocserverx86
    Opens key:
    Opens key:
                                                                  HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-
 00a0c9054228}\localserver32
                                                                  HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\localserver32
    Opens key:
    Opens kev:
                                                                  HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\inprochandler32
    Opens key:
                                                                 HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\inprochandler32
                                                                  HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-
    Opens key
 00a0c9054228}\inprochandlerx86
    Opens key:
                                                                  HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\ \ \ in prochandler x 86
    Opens key:
                                                                  HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\localserver
                                                                  HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\localserver
    Opens kev:
    Opens key:
                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\scrrun.dll
    Opens key:
                                                                  HKCU\software\classes\typelib
     Opens key:
                                                                  HKCR\typelib
    Opens key:
                                                                  HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-00a0c9054228}
    Opens key:
                                                                  HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}
    Opens key:
                                                                  HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0
    Opens key:
                                                                  HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0
    Opens key:
                                                                  HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-
00a0c9054228}\1.0\0
    Opens key:
                                                                  HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0
    Opens key:
                                                                  HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-
 00a0c9054228}\1.0\0\win32
    Opens key:
                                                                  HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0\win32
    Opens key:
                                                                  \label{thm:linear} \mbox{HKCU\software\wb and vba program settings\clock\sdata} \\
    Opens key:
                                                                  HKLM\system\currentcontrolset\control\session manager\appcertdlls
    Opens key:
                                                                  Opens key:
                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\apphelp.dll
    Opens key:
                                                                  HKLM\svstem\wpa\tabletpc
                                                                  HKLM\svstem\wpa\mediacenter
    Opens kev:
                                                                  HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
    Opens key:
                                                                  HKLM\software\microsoft\windows
    Opens key:
nt\currentversion\appcompatflags\custom\winjab.exe
                                                                  HKLM\software\policies\microsoft\windows\safer\levelobjects
    Opens key:
                                                                  \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} on the local density of the local densi
    Opens key:
    Opens key:
be2efd2c1a33}
                                                                  HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
    Opens kev:
    Opens key:
edd5fbde1328}
    Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes \setminus \{7fb9cd2e-3076-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57
b813f72dbb91}
    Opens key:
7c29ddecae3f}
    Opens key:
085bcc18a68d3
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-ae2e-4eb-4fe4-a
b91490411bfc}
    Opens key:
\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} is software \verb|\policies| microsoft| windows \end{tabular} is software \end{tabular} out of the local property 
    Opens key:
Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus hashes
    Opens key:
Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus paths
    Opens key:
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ \ 65536 \ has hes
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
    Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus paths
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
```

```
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
                                       HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus paths
  Opens key:
                                       HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
  Opens kev:
  Opens key:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \parbox{0.4cm} \end{tabular} \label{lem:hkcu}
  Opens key:
\label{local-condition} HKCU \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 4096 \ paths
  Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
  Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
  Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
\label{thm:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \normalised \norm
  Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus urlzones
  Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
                                       HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Opens key:
  Opens key:
                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winjab.exe
  Opens key:
                                       HKLM\software\microsoft\ctf\compatibility\winjab.exe
  Opens key:
                                       HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\1.bat
  Opens key:
                                       \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\cmd.exe
  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:
                                       HKCU\software\microsoft\windows\currentversion\internet settings
  Opens key:
                                       HKLM\software\policies
                                       HKCU\software\policies
  Opens key:
                                       HKCU\software
  Opens key:
  Opens key:
                                       HKLM\software
  Opens key:
                                       HKLM\software\policies\microsoft\internet explorer
                                       HKLM\software\policies\microsoft\internet explorer\main
  Opens key:
                                       HKLM\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
                                       HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
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
  Opens key:
                                       HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
  Opens key:
                                       HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
                                       HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\extensible cache
                                       HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\5.0\cache\extensible cache\domstore
                                       HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\extensible cache\feedplat
                                       HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\extensible cache\iecompat
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings \verb|\5.0| cache \verb|\extensible| cache \verb|\mshist012014033120140407|
  Opens key:
                                       \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \colongraph internet
settings \verb|\5.0| cache \verb|\extensible| cache \verb|\mshist012014041220140413|
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
  Opens key:
                                       HKCU\software\microsoft\internet
\verb|explorer\main\featurecontrol\retry_header on ly post\_on connection reset|\\
  Opens key:
                                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
```

HKCU\software\microsoft\internet

HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature bufferbreaking 818408

Opens key:

Opens key:

```
explorer\main\featurecontrol\feature_bufferbreaking_818408
                                   HKCU\software\microsoft\internet
  Opens kev:
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:
                                   \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\5.0\cache
  Opens key:
                                   HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
                                   HKCU\software\policies\microsoft\windows\system
  Opens kev:
                                   HKLM\software\microsoft\command processor
  Opens key:
                                   HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                                   HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
  Opens kev:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature use cname for spn kb911149
                                   HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:
                                   HKCU\software\microsoft\command processor
                                   HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
  Opens key:
                                  HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
  Opens key:
                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
  Opens key:
                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
  Opens key:
                                   HKLM\system\currentcontrolset\control\nls\locale
  Opens key:
                                   HKLM\system\currentcontrolset\control\nls\language groups
  Opens key
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
                                   HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
                                   HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
  Opens key:
                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                                   HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key:
                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key
                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
  Opens key:
                                   HKCU\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_passport\_check\_302\_for\_success\_kb949059
  Opens key:
                                  HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet settings\wpad
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
                                   HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens kev:
                                   HKLM\svstem\currentcontrolset\control\securityproviders
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet settings\cache
                                   HKCU\software\microsoft\internet explorer\lowregistry
  Opens kev:
  Opens key:
                                   HKLM\software\microsoft\windows
  Opens key:
                                   HKLM\software\microsoft\windows\html help
                                   HKLM\software\microsoft\windows\help
  Opens key:
  Opens key:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winjab.exe\rpcthreadpoolthrottle
  Oueries value:
                                   HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Oueries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [transparentenabled]
  Queries value:
                                   HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Oueries value:
                                   HKLM\software\microsoft\windows
nt \verb|\currentversion| compatibility 32[81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22]| to the state of the state o
                                  HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22]
                                   HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
  Queries value:
                                   HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
  Queries value:
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
  Queries value:
                                   {\tt HKLM \ } system \verb| current control set \verb| control \ \\ session
manager[criticalsectiontimeout]
                                   HKLM\software\microsoft\ole[rwlockresourcetimeout]
  Queries value:
  Queries value:
                                   HKCR\interface[interfacehelperdisableall]
  Queries value:
                                   HKCR\interface[interfacehelperdisableallforole32]
  Queries value:
                                   HKCR\interface[interfacehelperdisabletypelib]
  Queries value:
                                   HKCR\interface\{00020400-0000-0000-c000-
00000000046}[interfacehelperdisableall]
                                   HKCR\interface\{00020400-0000-0000-c000-
  Oueries value:
00000000046}[interfacehelperdisableallforole32]
                                  HKCU\control panel\desktop[multiuilanguageid]
HKLM\software\microsoft\ctf\systemshared[cuas]
  Oueries value:
  Oueries value:
                                   {\tt HKCU} \verb|keyboard layout \verb|toggle[language hotkey]|\\
  Queries value:
  Queries value:
                                   HKCU\keyboard layout\toggle[hotkey]
                                   HKCU\keyboard layout\toggle[layout hotkey]
  Oueries value:
```

```
Oueries value:
                                                  HKLM\software\microsoft\ctf[enableanchorcontext]
   Oueries value:
                                                  HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
   Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
   Queries value:
                                                  HKCU\software\microsoft\ctf[disable thread input manager]
   Oueries value:
                                                  HKLM\system\currentcontrolset\control\nls\codepage[932]
   Queries value:
                                                  HKLM\system\currentcontrolset\control\nls\codepage[949]
   Oueries value:
                                                  HKLM\system\currentcontrolset\control\nls\codepage[950]
   Oueries value:
                                                  HKLM \setminus system \setminus current control \setminus nls \setminus codepage [936]
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
   Oueries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
   Oueries value:
   Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
   Oueries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
   Oueries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
   Oueries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32\sqrtwave61
   Oueries value:
   Oueries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
   Oueries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
   Oueries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
   Queries value:
   Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
   Queries value:
   Oueries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
   Queries value:
   Queries 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]
   Queries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
   Queries value:
                                                  HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [midi9]
   Oueries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
   Oueries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
   Queries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
   Queries value:
   Queries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
   Queries value:
                                                  HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [aux 5]
   Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
   Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
   Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
   Queries value:
   Oueries value:
HKLM \label{lem:hklm} Whe all in the label lab
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
    Queries value:
   Queries value:
                                                  HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [mixer 1]
   Oueries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
   Oueries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
   Oueries value:
                                                  \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ drivers 32 [mixer 4]
   Oueries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
   Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
   Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
   Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
   Oueries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
   Oueries value:
                                                  HKLM\software\microsoft\com3[com+enabled]
   Oueries value:
                                                  HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
                                                  {\tt HKLM \setminus software \setminus microsoft \setminus ole[minimumfreemempercentage to create object]}
   Oueries value:
   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]
   Oueries value:
                                                  HKCR\clsid\{8856f961-340a-11d0-a96b-
   Oueries value:
00c04fd705a2}\inprocserver32[threadingmodel]
                                                  HKLM\system\setup[systemsetupinprogress]
   Queries value:
                                                  HKCU\control panel\desktop[smoothscroll]
   Queries value:
   Queries value:
HKCU \ software \ microsoft \ windows \ current version \ \ explorer \ \ advanced \ [enable balloon tips]
                                                  HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe[]
   Queries value:
   Oueries value:
                                                  HKLM\software\microsoft\internet explorer\setup[iexplorelastmodifiedlow]
   Queries value:
                                                  HKLM\software\microsoft\internet
explorer\setup[iexplorelastmodifiedhigh]
   Queries value:
                                                  HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
ab78-1084642581fb1
   Queries value:
                                                   HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
0000-0000000000001
   Oueries value:
                                                   HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib[]
   Queries value:
                                                   HKLM\software\microsoft\internet explorer\setup[installstarted]
                                                  HKCR \ interface \ \{b722bccb-4e68-101b-a2bc-00aa00404770\} \ proxystubclsid32[]
   Queries value:
                                                   HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32[]
   Queries value:
                                                  HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32[]
   Queries value:
                                                  HKCR \ interface \ \{93f2f68c-1d1b-11d3-a30e-00c04f79abd1\} \ proxystubclsid32[]
   Queries value:
   Queries value:
                                                  HKLM\software\microsoft\rpc[maxrpcsize]
   Queries value:
Queries value:
                                                  HKCR\clsid\{00021401-0000-0000-c000-
00000000046}\inprocserver32[inprocserver32]
   Queries value:
                                                  \label{locality} $$ HKCR\clsid_{00021401-0000-0000-c000-00000000046}\times\clsid_{00021401-0000-0000-c000-000000000046} $$ in processor of the content of the c
   Queries value:
                                                  HKCR\clsid\{00021401-0000-0000-c000-00000000046}[appid]
   Queries value:
                                                  HKCR\clsid\{00021401-0000-0000-c000-
00000000046}\inprocserver32[threadingmodel]
   Oueries value:
                                                  HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
  Oueries value:
                                                  HKLM\software\microsoft\internet
explorer \verb|\main| feature fea
   Oueries value:
                                                  HKLM\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature_protocol_lockdown[*]|
```

```
HKCR\clsid\{2087c2f4-2cef-4953-a8ab
 Oueries value:
66779b670495}\inprocserver32[inprocserver32]
 Oueries value:
                         HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\inprocserver32[]
 Oueries value:
                         HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}[appid]
 Queries value:
                         HKCR\clsid\{2087c2f4-2cef-4953-a8ab-
66779b670495}\inprocserver32[threadingmodel]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
 Oueries value:
                         HKLM\software\microsoft\windows\currentversion\internet
settings\connections[winhttpsettings]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
 Oueries value:
Queries value:
Oueries value:
HKL\\ M\system\current controlset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\common0000000003[packed catalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000004[packedcatalogitem]
 Queries value:
Queries value:
Oueries value:
Queries value:
Queries value:
Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Queries value:
Oueries value:
HKLM \ system \ current controls et \ services \ win sock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries \ 00000000001 \ [displaystring]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Oueries value:
Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ (catalog\_entries \ 0000000000001[enabled]) \ details a simple of the control set \ (catalog \ namespace\_catalog \ namespace\_cata
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001fstoresserviceclassinfol
 Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000002[displaystring]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_entries\000000000002[providerid]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000002[addressfamily]
 Oueries value:
Queries value:
Oueries value:
HKLM \ system \ current control set \ services \ \ winsock 2 \ parameters \ namespace\_catalog 5 \ \ catalog\_entries \ \ 0000000000002 \ [version]
 Queries value:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 0000000000002 [storesserviceclass info]]
  Queries value:
Queries value:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries \ 00000000000003 \ [displaystring]
 Queries value:
HKLM \ system \ current controls et \ services \ \ winsock 2 \ parameters \ namespace\_catalog 5 \ \ catalog\_entries \ \ 000000000003 \ [providerid]
 Queries value:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ namespace\_catalog5 \ (catalog\_entries \ 00000000003 \ [address family]
 Queries value:
Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
 Oueries value:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries \ 00000000003 \ [storesserviceclassinfo]
 Oueries value:
```

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

Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount] Oueries value: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ rpc\+ security service\+ [default authlevel]$ Oueries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername] Oueries value: HKLM\svstem\currentcontrolset\services\tcpip\parameters[disableadapterdomainname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] Queries value: $\label{lem:hklm} \verb+Kklm/system/currentcontrolset/services/tcpip/parameters[allowunqualified query]+ \\$ Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [register adapter name]$ Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Oueries value: $HKLM \verb|\system| current controlset \verb|\services| dnscache \verb|\parameters[registerreverselookup]|$ Oueries value: Queries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[registerwanadapters] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandvnamicupdate] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Queries value: $\label{local-parameters} $$HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]$$$ Oueries value: Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [updates ecurity level]$ Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [update zone exclude file]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [max cachettl]$ Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [maxnegative cachettl]$ Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [adapter time out limit]$ Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts] Oueries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind] Oueries value: $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4303-abe3-4304-a$ c7d49d7cecdc}[enabledhcp] Oueries value: $\label{local-equation} \begin{tabular}{ll} HKLM \end{tabular} A the control set \end{tabular} $$ HKLM \end{tabular} are the control set \end{tabular} $$ A the control set \end{tabular} $$ A$ c7d49d7cecdc}[leaseobtainedtime] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[leaseterminatestime] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[dhcpserver] HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] Queries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain] Queries value: c7d49d7cecdc}[queryadaptername] Oueries value: c7d49d7cecdc}[disableadapterdomainname] c7d49d7cecdc}[registrationenabled] Queries value: c7d49d7cecdc}[registeradaptername] Queries value: c7d49d7cecdc}[registrationmaxaddresscount] Oueries value: c7d49d7cecdc}[maxnumberofaddressestoregister] Queries value: c7d49d7cecdc}[domain] Queries value: $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-a$ c7d49d7cecdc}[dhcpdomain] Queries value: c7d49d7cecdc}[ipautoconfigurationenabled] Oueries value: c7d49d7cecdc}[addresstype] Oueries value: c7d49d7cecdc}[nameserver] Oueries value: c7d49d7cecdc}[dhcpnameserver] HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder] Queries value: $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM\software\mbox{$\stackrel{\cdot}{\rm microsoft}$ cryptography\defaults\provider\mbox{$\stackrel{\cdot}{\rm microsoft}$ strong} \end{tabular}$ cryptographic provider[type] HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong Queries value: cryptographic provider[image path] Queries value: HKLM\software\microsoft\cryptography[machineguid] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll] Oueries value: HKCR\scripting.filesystemobject\clsid[] HKCR\clsid\{0d43fe01-f093-11cf-8940-Queries value: 00a0c9054228}\inprocserver32[inprocserver32] HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\inprocserver32[] Queries value: HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}[appid] Oueries value: HKCR\clsid\{0d43fe01-f093-11cf-8940-Oueries value: 00a0c9054228}\inprocserver32[threadingmodel] HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0\win32[] Queries value: HKLM\system\currentcontrolset\control\session Queries value: manager\appcompatibility[disableappcompat] HKLM\system\wpa\mediacenter[installed] Queries value: Queries value:

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

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

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

Queries value:

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

Queries value:

Queries value:

 $\label{thm:local-basis} HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328\}[hashalg]}$

```
Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemsize]
   Queries value:
edd5fbde1328}[saferflags]
   Queries value:
b813f72dbb91}[itemdata]
   Oueries value:
b813f72dbb91}[hashalg]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[itemsize]
   Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[saferflags]
   Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemdata]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[hashalg]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemsize]
   Queries value:
7c29ddecae3f}[saferflags]
   Oueries value:
085bcc18a68d}[itemdata]
   Queries value:
085bcc18a68d}[hashalg]
085bcc18a68d}[itemsize]
   Queries value:
085bcc18a68d}[saferflags]
   Queries value:
b91490411bfc}[itemdata]
   Oueries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes \setminus \{dc971ee5-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2
b91490411bfc}[hashalg]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemsize]
   Oueries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes \setminus \{dc971ee5-44eb-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2e-4fe4-ae2
b91490411bfc}[saferflags]
   Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
   Oueries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [policy scope]
                                              HKCU\software\microsoft\windows\currentversion\explorer\shell
   Oueries value:
folders[cache]
   Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
                                              HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\compatibility32[winjab]
                                              HKLM\software\microsoft\windows nt\currentversion\ime
   Queries value:
compatibility[winjab]
   Queries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
                                              HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[secureprotocols]
   Queries value:
                                              HKLM\software\policies\microsoft\internet
explorer\main[security_hklm_only]
   Oueries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
   Queries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
   Queries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
   Queries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
                                              HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[cachemode]
   Queries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
   Queries value:
                                              \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings[proxyhttp1.1]
   Queries value:
                                              \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings[enablenegotiate]
                                              \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
   Oueries value:
settings[disablebasicoverclearchannel]
   Oueries value:
                                              HKCU\software\microsoft\internet
{\tt explorer} \verb|\main| feature control[feature\_client author tfilter]|
```

HKLM\software\microsoft\internet

explorer\main\featurecontrol[feature_clientauthcertfilter]

Oueries value:

```
HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[clientauthbuiltinui]
  Oueries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
                                   \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \begin{tabular}{ll} software \begin{tabular}{ll} microsoft \begin{tabular}{ll} windows \begin{tabular}{ll} current version \begin{tabular}{ll} internet \begin{tabular}{ll} current \begin{tabular}
  Queries value:
{\tt settings \ \ 5.0 \ \ } cache [session start time default delta secs]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[signature]
  Oueries 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]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
  Oueries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cacheprefix]
  Oueries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cachelimit]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\cookies[peruseritem]
                                   HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\cookies[peruseritem]
                                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Oueries value:
folders[cookies]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\cookies[cacheprefix]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cachelimit]
                                   \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current \+ version \+ internet
  Queries value:
settings\5.0\cache\history[peruseritem]
  Oueries value:
                                   HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\history[cachelimit]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\domstore[cacherepair]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachepath]
                                   \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
  Queries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\domstore[cachelimit]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheoptions]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacherepair]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
  Oueries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
  Oueries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacherepair]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Oueries 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]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\ietld[cacherepair]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
  Oueries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]
                                   \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
  Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings \verb|\|5.0| cache \verb|\|extensible| cache \verb|\|mshist012014033120140407[cache options]|
  Oueries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
  Oueries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
  Oueries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
```

settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]

```
HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
                           \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cacherepair]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\compatibility32[cmd]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\ime compatibility[cmd]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disableworkerthreadhibernation]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablereadrange]
                           \label{thm:local_hammon_hammon} \mbox{HKCU\software\mbox{\sc microsoft\windows\currentversion\sc internet}} \\
 Oueries value:
settings[socketsendbufferlength]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketreceivebufferlength]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[keepalivetimeout]
                           \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current \+ version \+ internet
 Queries value:
settings[maxhttpredirects]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1 Oserver]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings[maxconnectionsperproxy]
                           \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current \+ version \+ internet
 Queries value:
settings[serverinfotimeout]
                           \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
 Queries value:
settings[connecttimeout]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connecttimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[connectretries]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendtimeout]
 Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[receivetimeout]
 Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablentlmpreauth]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[scavengecachelowerbound]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[certcachenovalidate]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelifetime]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
                           HKLM\software\microsoft\command processor[disableunccheck]
 Oueries value:
 Queries value:
                           HKLM\software\microsoft\command processor[enableextensions]
 Queries value:
                           HKLM\software\microsoft\command processor[delayedexpansion]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Oueries value:
                           HKLM\software\microsoft\command processor[defaultcolor]
  Queries value:
                           {\tt HKLM \setminus software \setminus microsoft \setminus command processor[completion char]}
                           HKLM\software\microsoft\command processor[pathcompletionchar]
  Queries value:
  Queries value:
                           HKLM\software\microsoft\command processor[autorun]
                           {\tt HKCU \backslash software \backslash microsoft \backslash command processor[disable unccheck]}
  Queries value:
                           HKCU\software\microsoft\command processor[enableextensions]
  Queries value:
  Queries value:
                           HKCU\software\microsoft\command processor[delayedexpansion]
                           HKCU\software\microsoft\command processor[defaultcolor]
 Queries value:
                           HKCU\software\microsoft\command processor[completionchar]
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[httpdefaultexpirytimesecs]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value
settings[ftpdefaultexpirytimesecs]
 Queries value:
                           HKCU\software\microsoft\command processor[pathcompletionchar]
  Queries value:
                           {\tt HKCU \backslash software \backslash microsoft \backslash command \ processor[autorun]}
 Oueries value:
                           HKLM\system\currentcontrolset\control\nls\locale[00000409]
 Oueries value:
                           Oueries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe]
 Oueries value:
                           HKLM\software\microsoft\internet
```

explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]

```
HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[disablecachingofsslpages]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
                                      \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
  Queries value:
settings[leashlegacycookies]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[disablent4rascheck]
  Oueries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Oueries value:
                                      HKLM\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
  Oueries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[bypassftptimecheck]
  Oueries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduringauth]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[releasesocketduring401auth]
                                      HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[releasesocketduring401auth]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[wpadsearchalldomains]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablelegacypreauthasserver]
                                      HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablelegacypreauthasserver]
                                      \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current \+ version \+ internet
  Queries value:
settings[bypasshttpnocachecheck]
  Oueries value:
                                      \label{lem:hklm} \verb+Kklm\+ software\+ incressft\+ windows\+ current version\+ internet
settings[bypasshttpnocachecheck]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
                                      HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasssslnocachecheck]
  Queries value
                                      HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
                                      \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings[nocheckautodialoverride]
                                      \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings[nocheckautodialoverride]
                                      \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \c
  Queries value:
settings[dontusednsloadbalancing]
                                      HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dontusednsloadbalancing]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
  Oueries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonpost]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnalwaysonpost]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonzonecrossing]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnonbadcertsending]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnonbadcertrecving]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnonpostredirect]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[alwaysdrainonredirect]
  Queries value:
                                      \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current \+ version \+ internet
settings[warnonhttpstohttpredirect]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[globaluseroffline]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
  Queries value:
                                      HKLM\software\microsoft\windows\currentversion\internet
settings[urlencoding]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[truncatefilename]
                                      \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings[badproxyexpirestime]
  Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
                                      \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
  Queries value:
settings\cache[persistent]
  Queries value:
                                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[winjab.exe]
  Sets/Creates value:
                                      HKCU\software\microsoft\windows\currentversion\run[wincl]
  Sets/Creates value:
                                      HKCU\software\vb and vba program settings\clock\sdata[s]
  Value changes:
                                      HKLM\software\microsoft\cryptography\rng[seed]
  Value changes:
                                      \label{local-constraint} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\shell}} \\
folders[cache]
  Value changes:
                                      HKCU\software\microsoft\windows\currentversion\explorer\shell
```

folders[cookies]
 Value changes:
folders[history]

HKCU\software\microsoft\windows\currentversion\explorer\shell