Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 627, Task ID: 2454

Task ID: 2454

Risk Level:

Date Processed: 2016-02-22 05:32:20 (UTC)

Processing Time: 60.0 seconds IntelliVM Virtual Environment:

Execution Arguments:

c:\windows\temp\d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exe"

627 Sample ID: Type: basic Owner:

d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174 Label:

Date Added: 2016-02-22 05:26:50 (UTC) File Type: PE32:win32:gui File Size: 327744 bytes

MD5: 08c1a0627200a235be2709d4ef702f3f

SHA256: d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174

Description:

Pattern Matching Results

5 Creates process in suspicious location

3 Connects to local host

2 PE: Nonstandard section

6 Writes to system32 folder 6 Dumps and runs batch script

5 Creates file in drivers folder

Static Events

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

Process/Thread Events

Creates process:

C:\WINDOWS\Temp\d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exe ["c:\windows\temp\d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exe"]

C:\WINDOWS\system32\cmd.exe [cmd /c Creates process:

C:\DOCUME~1\Admin\LOCALS~1\Temp\gtnctie.bat]

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

["C:\DOCUME~1\Admin\LOCALS~1\Temp\wqwgdy.exe"]

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

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

Creates mutex:

\BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-

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

settings!temporary internet files!content.ie5!

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

settings!history!history.ie5!

Creates mutex: \BaseNamedObjects\WininetConnectionMutex \BaseNamedObjects\ZonesCounterMutex Creates mutex:

Creates mutex: \BaseNamedObjects\ZoneAttributeCacheCounterMutex Creates mutex: \BaseNamedObjects\ZonesCacheCounterMutex Creates mutex: \BaseNamedObjects\ZonesLockedCacheCounterMutex Creates event: \BaseNamedObjects\userenv: User Profile setup event

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

File System Events

Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\gtnctie.bat</pre>
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\xfltuz.bat</pre>
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\wqwgdy.exe

Creates: C:\WINDOWS\system32\byeqcvy.dll Creates C:\WINDOWS\system32\drivers\bnq.sys

C:\WINDOWS\Prefetch\D488539402ABAE3873B801373DBC8-136C5A2A.pf Opens:

Opens: C:\Documents and Settings\Admin C:\WINDOWS\system32\imm32.dll Opens: C:\WINDOWS\system32\shell32.dll Opens:

C:\WINDOWS\system32\SHELL32.dll.124.Manifest Opens: C:\WINDOWS\system32\SHELL32.dll.124.Config Opens: C:\WINDOWS\WinSxS\x86 Microsoft.Windows.Common-Opens:

Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83

C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Opens:

Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll

```
Opens:
                          C:\WINDOWS\WindowsShell.Manifest
                          C:\WINDOWS\WindowsShell.Config
 Opens:
                          C:\WINDOWS\system32\comctl32.dll
 Opens:
 Opens:
                          C:\WINDOWS\system32\comctl32.dll.124.Manifest
 Opens:
                          C:\WINDOWS\system32\comctl32.dll.124.Config
                          C:\WINDOWS\system32\urlmon.dll.123.Manifest
 Opens:
                          C:\WINDOWS\system32\urlmon.dll.123.Config
 Opens:
                          C:\WINDOWS\system32\MSCTF.dll
 Opens:
 Opens:
                          C:\WINDOWS\system32\MSCTFIME.IME
                          C:\Documents and Settings\Admin\Local Settings\Temp
C:\Documents and Settings\Admin\Local Settings\Temp\gtnctie.bat
 Opens:
 Opens:
                          C:\WINDOWS\system32\apphelp.dll
 Opens:
                          C:\WINDOWS\AppPatch\sysmain.sdb
 Opens:
                          C:\WINDOWS\AppPatch\systest.sdb
 Opens:
 Opens:
                          C:\
 Opens:
                          C:\Documents and Settings
 Opens:
                          C:\Documents and Settings\Admin\Local Settings
 Opens:
                          C:\WINDOWS\system32\cmd.exe
 Opens:
                          C:\WINDOWS\system32\cmd.exe.Manifest
 Opens:
                          C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf
 Opens:
                          C:\WINDOWS
 Opens:
                          C:\WINDOWS\AppPatch
 Opens:
 Opens:
                          C:\WINDOWS\system32
 Opens:
                          C:\WINDOWS\system32\wbem
                          C:\WINDOWS\WinSxS
 Opens:
                          C:\WINDOWS\system32\ntdll.dll
 Opens:
 Opens:
                          C:\WINDOWS\system32\kernel32.dll
 Opens:
                          C:\WINDOWS\system32\unicode.nls
                          C:\WINDOWS\system32\locale.nls
 Opens
                          C:\WINDOWS\system32\sorttbls.nls
 Opens
 Opens:
                          C:\WINDOWS\system32\msvcrt.dll
 Opens:
                          C:\WINDOWS\system32\user32.dll
 Opens:
                          C:\WINDOWS\system32\gdi32.dll
                          C:\WINDOWS\system32\shimeng.dll
 Opens:
 Opens:
                          C:\WINDOWS\AppPatch\AcGenral.dll
 Opens:
                          C:\WINDOWS\system32\advapi32.dll
 Opens:
                          C:\WINDOWS\system32\rpcrt4.dll
 Opens:
                          C:\WINDOWS\system32\secur32.dll
 Opens:
                          C:\WINDOWS\system32\winmm.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:
                          C:\WINDOWS\system32\shlwapi.dll
                          C:\WINDOWS\system32\userenv.dll
 Opens:
                          {\tt C:\WINDOWS\system32\uxtheme.dll}
 Opens:
                          C:\WINDOWS\system32\ctype.nls
 Opens:
                          C:\WINDOWS\system32\sortkey.nls
 Opens:
                          C:\WINDOWS\system32\wbem\wmic.exe
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\Temp\xfltuz.bat
 Opens:
                          C:\WINDOWS\Temp\f9166da0-ddb1-4fae-85c2-770eb3858939
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\Temp\tmpyvpur.bat
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\Temp\wqwgdy.exe
 Opens:
                          C:\DOCUME~1\Admin\LOCALS~1\Temp\wqwgdy.exe.Manifest
C:\WINDOWS\Prefetch\WQWGDY.EXE-056C36A3.pf
 Opens:
 Opens:
                          C:\WINDOWS\system32\dbghelp.dll
 Opens:
 Opens:
                          C:\WINDOWS\system32\WININET.dll.123.Manifest
                          C:\WINDOWS\system32\WININET.dll.123.Config
 Opens:
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\History
                          C:\Documents and Settings\Admin\Local Settings\History\History.IE5
 Opens:
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
 Opens:
                          C:\Documents and Settings\Admin\Cookies
                          C:\Documents and Settings\Admin\Cookies\index.dat
 Opens:
                          C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\index.dat
                          C:\WINDOWS\system32\ws2_32.dll
                          C:\WINDOWS\system32\ws2help.dll
 Opens:
                          C:\WINDOWS\system32\rasapi32.dll
 Opens:
                          C:\WINDOWS\system32\rasman.dll
 Opens:
 Opens:
                          C:\WINDOWS\system32\netapi32.dll
 Opens:
                          C:\WINDOWS\system32\tapi32.dll
 Opens:
                          C:\WINDOWS\system32\rtutils.dll
 Opens:
                          C:\WINDOWS\system32\TAPI32.dll.124.Manifest
 Opens:
                          C:\WINDOWS\system32\TAPI32.dll.124.Config
 Opens:
                          C:\AUTOEXEC.BAT
                          C:\Documents and Settings\All Users\Application
 Opens:
Data\Microsoft\Network\Connections\Pbk
 Opens:
                          C:\WINDOWS\system32\ras
 Opens:
                          C:\Documents and Settings\Admin\Application
Data\Microsoft\Network\Connections\Pbk\
                          C:\WINDOWS\system32\sensapi.dll
 Opens:
                          C:\WINDOWS\system32\mswsock.dll
 Opens:
                          C:\WINDOWS\system32\hnetcfg.dll
 Opens:
                          C:\WINDOWS\system32\wshtcpip.dll
 Opens:
                          C:\WINDOWS\system32\byeqcvy.dll
 Opens:
                          C:\WINDOWS\system32\drivers
 Opens:
                          C:\WINDOWS\system32\msv1_0.dll
 Opens:
 Opens:
                          C:\WINDOWS\system32\iphlpapi.dll
```

C:\WINDOWS\system32\rasadhlp.dll

Opens:

Opens: C:\WINDOWS\system32\dnsapi.dll Opens: C:\WINDOWS\system32\drivers\etc\hosts Opens: C:\WINDOWS\system32\rsaenh.dll

 ${\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\wqwgdy.exe}$ Writes to: Writes to: ${\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\xfltuz.bat}$ Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\gtnctie.bat

Writes to: C:\WINDOWS\system32\byeqcvy.dll Writes to: C:\WINDOWS\system32\drivers\bnq.sys Reads from: C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf

 ${\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\gtnctie.bat}$ Reads from: Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\xfltuz.bat

C:\AUTOEXEC.BAT Reads from:

Reads from: C:\WINDOWS\system32\drivers\etc\hosts Reads from: C:\WINDOWS\system32\rsaenh.dll

C:\Documents and Settings\Admin\Local Settings\Temp\xfltuz.bat Deletes:

Network Events

Connects to: 127.0.0.1:1044

Windows Registry Events

Creates key: HKLM\software\microsoft\windows\currentversion\datetime

Creates kev: HKLM\software\microsoft\downloadmanager

Creates key: HKCU\software\microsoft\windows\currentversion\internet settings Creates key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders

HKCU\software\microsoft\windows\currentversion\explorer\shell folders Creates key

Creates kev: HKLM\software\microsoft\tracing

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

folders

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

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

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

settings\connections

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

awareness

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

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

options\d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exe Opens key: HKLM\system\currentcontrolset\control\terminal server

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

options\gdi32.dll

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

options\user32.dll

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

Opens key: Opens key: $HKLM \verb|\software\policies\microsoft\windows\safer\code identifiers$

Opens key: $\label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ safer\+ code identifiers$ Opens key: $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constraint of the constr$ options\imm32.dll

Opens key:

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

Opens key:

Opens key:

Opens kev:

Opens key:

options\ole32.dll Opens key:

options\oleaut32.dll Opens key:

options\iertutil.dll Opens key:

HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\secur32.dll

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

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

options\advapi32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll

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

options\shlwapi.dll HKLM\software\microsoft\windows nt\currentversion\image file execution options\shell32.dll

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

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

options\urlmon.dll Opens key: HKLM\system\currentcontrolset\control\error message instrument\ Opens key: $\label{lem:hklm} \verb+Kklm \system \current control \set \control \set ror message instrument$ Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32 Opens kev: HKLM\software\microsoft\windows nt\currentversion\ime compatibility

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

HKLM\ Opens key:

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

HKLM\system\setup Opens key:

HKCU\ Opens key:

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

```
Opens key:
                                                                              HKCU\control panel\desktop
     Opens key:
HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} windows \label{lem:hklm} current version \label{lem:hklm} \label{lem:hklm} Software \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hkklm} HKLM \label{lem:hkklm} \label{lem:hkklm} Software \label{lem:hkklm} \label{le
     Opens key:
                                                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\comctl32.dll
     Opens key:
                                                                              \label{thm:linear} \verb+HKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ advanced
     Opens key:
                                                                              HKLM\software\microsoft\windows nt\currentversion\languagepack
     Opens key:
                                                                              HKLM\software\microsoft\ole
     Opens key:
                                                                              HKCR\interface
                                                                              HKCR\interface\{00020400-0000-0000-0000-0000000000046}
     Opens kev:
                                                                              HKLM\software\microsoft\oleaut
     Opens key:
     Opens key:
                                                                              HKLM\software\microsoft\oleaut\userera
     Opens key:
                                                                              HKCU\software\classes\
     Opens key:
                                                                              HKCU\software\classes\protocols\name-space handler\
                                                                              HKCR\protocols\name-space handler
     Opens key:
                                                                              HKCU\software\classes\protocols\name-space handler
     Opens kev:
     Opens key:
                                                                              HKCU\software\policies\microsoft\windows\currentversion\internet
settings
     Opens kev:
                                                                              HKLM\software\microsoft\windows\currentversion\internet settings
     Opens key:
                                                                              HKLM\software\policies\microsoft\windows\currentversion\internet
settings
     Opens key:
                                                                              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
                                                                             HKLM\software\microsoft\internet
     Opens key:
 explorer\main\featurecontrol\feature_protocol_lockdown
                                                                              HKLM\software\policies\microsoft\windows\currentversion\internet
     Opens key:
settings\
     Opens key:
                                                                              \label{lem:hklmsoftware policies microsoft} Internet explorer \verb|\main| feature control| \\
     Opens key:
                                                                              \label{lem:hkcu} \verb+KKCU\+ software \verb+\policies+ microsoft+ internet explorer+ main+ feature control
     Opens key:
                                                                              HKLM\software\microsoft\internet explorer\main\featurecontrol
                                                                              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\
                                                                              HKCU\software\policies\microsoft\windows\currentversion\internet
     Opens key:
 settings\zonemap\domains\
     Opens key:
                                                                             HKLM\software\policies\microsoft\windows\currentversion\internet
 settings\zonemap\ranges\
                                                                              \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
     Opens key:
 settings\zonemap\ranges\
     Opens key:
                                                                             HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_unc_savedfilecheck
     Opens key:
                                                                              HKLM\software\microsoft\internet
 explorer\main\featurecontrol\feature_unc_savedfilecheck
     Opens key:
                                                                              \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constraint of the constr
options\msctf.dll
     Opens key:
HKLM \setminus software \setminus microsoft \setminus cff \setminus compatibility \setminus d488539402 abae 3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exection (a) the software \setminus microsoft \setminus cff \setminus compatibility \setminus d488539402 abae 3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exection (a) the software \setminus microsoft \setminus cff \setminus compatibility \setminus d488539402 abae 3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exection (a) the software \setminus microsoft \setminus cff \setminus c
     Opens key:
                                                                              HKLM\software\microsoft\ctf\systemshared\
     Opens key:
                                                                              HKCU\keyboard layout\toggle
     Opens key:
                                                                              HKLM\software\microsoft\ctf\
     Opens key:
                                                                              HKLM\software\microsoft\windows nt\currentversion\imm
     Opens key:
                                                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
     Opens key:
                                                                              HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
     Opens kev:
                                                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\msctfime.ime
                                                                              HKCU\software\microsoft\ctf
     Opens kev:
     Opens key:
                                                                              HKLM\software\microsoft\ctf\systemshared
     Opens key:
                                                                              HKCU\software\microsoft\internet explorer\main
     Opens key:
                                                                              HKLM\system\currentcontrolset\control\session manager\appcompatibility
     Opens key:
                                                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\apphelp.dll
     Opens key:
                                                                              HKLM\system\wpa\tabletpc
     Opens key:
                                                                              HKLM\system\wpa\mediacenter
     Opens kev:
                                                                              HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
     Opens key:
                                                                              HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\gtnctie.bat
     Opens key:
                                                                              HKLM\software\policies\microsoft\windows\safer\levelobjects
     Opens kev:
                                                                              HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
     Opens kev:
be2efd2c1a33}
      Opens key:
                                                                              Opens key:
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{349d35ab-37b5-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-46666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-46666f-9b89-4666f-9b89-46666f-9b89-46666
 edd5fbde1328}
     Opens key:
b813f72dbb91}
      Opens key:
7c29ddecae3f}
     Opens key:
085bcc18a68d3
     Opens key:
b91490411bfc}
     Opens key:
```

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

```
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
    Opens kev:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus urlzones
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
    Opens kev:
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 kev:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
    Opens key:
                                                               HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
    Opens key:
                                                               HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
    Opens key:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \parbox{0.4mm} \code id
    Opens key:
HKCU \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ \ 4096 \ paths
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
    Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus urlzones
    Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
     Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
    Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus urlzones
     Opens key:
\label{local-eq:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \normalle 131072 \paths \normalle 121072 \paths \normalle 12
    Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus has hes
    Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
    Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus paths
    Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
    Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
                                                               HKCU\software\microsoft\windows\currentversion\explorer\shell folders
    Opens key:
    Opens key:
                                                               HKLM\svstem\currentcontrolset\control\session manager\appcertdlls
    Opens key:
                                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cmd.exe
    Opens key:
                                                               HKCU\software\policies\microsoft\windows\system
    Opens key:
                                                               HKLM\software\microsoft\command processor
    Opens kev:
                                                               HKCU\software\microsoft\command processor
    Opens kev:
                                                               HKLM\system\currentcontrolset\control\nls\locale
    Opens key:
                                                               HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
    Opens key:
                                                               HKLM\system\currentcontrolset\control\nls\language groups
    Opens key:
                                                               HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\wgwgdy.exe
    Opens key:
                                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wqwgdy.exe
    Opens key:
                                                               HKCU\software\microsoft\windows\currentversion\internet settings
    Opens key:
                                                               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
    Opens key:
                                                               HKLM\software\microsoft\internet
 explorer\main\featurecontrol\feature_http_username_password_disable
    Opens key:
                                                               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
    Opens kev:
                                                               HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_allow\_reverse\_solidus\_in\_userinfo\_kb932562
                                                               HKCU\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
                                                               HKLM\software\microsoft\internet
    Opens key:
 explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
    Opens key:
                                                               HKCU\software\microsoft\internet explorer\ietld
    Opens key:
                                                               HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_mime_handling
    Opens key:
                                                              HKLM\software\microsoft\internet
 explorer\main\featurecontrol\feature_mime_handling
    Opens key:
                                                               \label{lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem:http-lem
    Opens key:
                                                               HKCR\protocols\name-space handler\http
    Opens key:
                                                               HKCU\software\classes\protocols\name-space handler\*\
```

HKCR\protocols\name-space handler*

HKCU\software\microsoft\internet

Opens key:

Opens key:

```
Opens key:
                                    HKLM\software\microsoft\windows\currentversion\internet settings\user
agent
  Opens key:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent
  Opens key:
                                     HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent
  Opens key:
                                    HKLM\software\policies
  Opens key:
                                    HKCU\software\policies
  Opens key:
                                    HKCU\software
  Opens kev:
                                    HKLM\software
                                    HKLM\software\microsoft\windows\currentversion\internet settings\user
  Opens key:
agent\ua tokens
  Opens key:
                                     HKLM\software\microsoft\windows\currentversion\internet settings\user
agent\pre platform
  Opens kev:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\pre platform
                                    HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\5.0\user agent\pre platform
  Opens key:
                                    HKLM\software\microsoft\windows\currentversion\internet settings\user
agent\post platform
  Opens key
                                    HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\post platform
  Opens kev:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\post platform
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
  Opens key:
                                    \label{lem:hklmsoftware} \verb+MKLM+ software+ \verb+microsoft+ windows nt+ current version+ image file execution
options\normaliz.dll
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wininet.dll
  Opens key:
                                     HKLM\system\currentcontrolset\control\wmi\security
  Opens key:
                                     HKLM\software\policies\microsoft\internet explorer
  Opens key:
                                    HKLM\software\policies\microsoft\internet explorer\main
  Opens key:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache
                                    HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache
  Opens key:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
                                    \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
  Opens key:
settings\5.0\cache\content
  Opens key:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
  Opens key:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
  Opens key:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
  Opens key:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
  Opens key:
                                    HKLM\software\microsoft\rpc\pagedbuffers
  Opens key:
                                    HKLM\software\microsoft\rpc
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens kev:
options \verb|\| d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exe \verb|\| rethreadpoolthrottle| and the second of the second of
  Opens key:
                                    HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:
                                    HKLM\system\currentcontrolset\control\computername
  Opens key:
                                    HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens kev:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache
                                    HKCU\software\microsoft\windows\currentversion\internet
  Opens key
settings\5.0\cache\extensible cache\domstore
                                    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\5.0\cache\extensible cache\mshist012014033120140407
  Opens key:
                                    \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current \+ version \+ internet
settings\5.0\cache\extensible cache\mshist012014041220140413
  Opens key:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
  Opens key:
                                    HKCU\software\microsoft\internet
explorer \verb|\main| feature control| retry_header on ly post\_on connection reset
  Opens key:
                                    HKLM\software\microsoft\internet
\verb|explorer| \verb|main| feature control| retry_header on lypost\_on connection reset| \\
                                    HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_bufferbreaking_818408
                                    HKLM\software\microsoft\internet
  Opens key
explorer\main\featurecontrol\feature_bufferbreaking_818408
                                    HKCU\software\microsoft\internet
  Opens key
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  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
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
  Opens key:
                                    HKLM\software\microsoft\internet
```

 $explorer \verb|\main| featurecontrol| feature_fix_chunked_proxy_script_download_kb843289$

```
Opens key:
                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:
                                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:
                                        HKCU\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature\_use\_spn\_for\_ntlm\_auth\_disabled|\\
  Opens key:
                                        HKLM\software\microsoft\internet
explorer \verb|\main\featurecontrol\feature\_use\_spn\_for\_ntlm\_auth\_disabled|
  Opens key:
                                        HKCU\software\microsoft\internet
\verb|explorer| \verb|main| featurecontrol| feature_allow_long_international\_file names| \\
  Opens kev:
                                        HKLM\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature\_allow\_long\_international\_file names| \\
  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
                                        HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
  Opens kev:
                                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
  Opens key:
                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
  Opens kev:
                                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
  Opens key:
                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key:
                                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key:
                                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
  Opens kev:
                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
                                        HKLM\software\microsoft\internet
  Opens key:
explorer \verb|\main| featurecontrol| feature_passport\_check\_302\_for\_success\_kb949059
  Opens key:
                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
  Opens key:
                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
  Opens key:
                                        HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus protocol\_catalog 9
  Opens key:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ 00000004
  Opens key
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol\_catalog \ catalog\_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
  Opens key:
Opens key:
Opens key:
Opens key:
Opens key:
                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dbghelp.dll
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000006
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000007
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\0000000000000
  Opens key:
Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
Opens key:
Opens key:
HKCU\software\microsoft\windows\currentversion\internet settings\wpad
  Opens key:
  Opens key:
                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:
                                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:
                                        \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constraint of the constr
options\netapi32.dll
  Opens key:
                                        \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constraint of the constr
options\rasman.dll
  Opens key:
                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rtutils.dll
  Opens key:
                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winmm.dll
```

Opens key: HKLM\software\microsoft\windows nt\currentversion\drivers32 Opens key: $\label{lem:hklm} \verb+Kklm \+ system \+ current control \+ edia properties \+ private properties \+ joystick \+ winmm \+ in the lem \+ current \+ control \+ respective \+ private \+ privat$ Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\tapi32.dll Opens key: HKLM\software\microsoft\windows\currentversion\telephony Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasapi32.dll Opens key: HKLM\software\microsoft\tracing\rasapi32 Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution options\userenv.dll Opens key: HKLM\system\currentcontrolset\control\productoptions Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders Opens key: HKLM\software\policies\microsoft\windows\system HKLM\software\microsoft\windows nt\currentversion\profilelist Opens kev: HKLM\system\currentcontrolset\control\session manager\environment Opens kev: Opens kev: HKLM\software\microsoft\windows\currentversion Opens key: HKU\ HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-Opens key: 1757981266-507921405-1957994488-1003 HKCU\environment Opens key: Opens key: HKCU\volatile environment Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\sensapi.dll Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_maxconnectionsperserver Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_maxconnectionsperserver Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_maxconnectionsper1_0server Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_maxconnectionsper1_0server Opens key: HKCU\software\microsoft\windows\currentversion\urlmon settings Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\http filters\rpa Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\http filters\rpa Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_include_port_in_spn_kb908209 HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_include_port_in_spn_kb908209 Opens key: $\label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\$ settings\zonemap\ Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\ranges\ HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\zonemap\protocoldefaults\ Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\domains\ HKLM\software\microsoft\windows\currentversion\internet Opens key: settings\zonemap\domains\ HKLM\software\microsoft\windows\currentversion\internet Opens kev: settings\zonemap\domains\msn.com HKLM\software\microsoft\windows\currentversion\internet Opens kev: settings\zonemap\domains\msn.com\related HKLM\software\policies\microsoft\internet explorer\security Opens kev: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mswsock.dll Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\ Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\ Opens key: $\label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ settings\zones\ Opens kev: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\0 HKCU\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zones\0 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\1 Opens key: $\label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ settings\zones\1 Opens key: $\label{lem:hklm} \verb+Kklm \+ software \+ policies \+ microsoft \+ windows \+ current \+ version \+ internet$ settings\zones\2 Opens key: $\label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ settings\zones\2 Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ settings\zones\3 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\3 HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zones\4

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

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

Opens key:

settings\zones\4 Opens key:

```
options\hnetcfg.dll
   Opens key:
                                               HKLM\software\microsoft\rpc\securityservice
   Opens key:
                                               HKLM\system\currentcontrolset\services\winsock\parameters
   Opens key:
                                               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
   Opens key:
                                               HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
   Opens key:
                                               \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\
   Opens key:
                                               HKLM\svstem\currentcontrolset\services\tcpip\parameters\winsock
   Opens kev:
                                               HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
   Opens key:
                                               HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown zones\
                                              \label{thm:local_hammon_hammon} \mbox{HKCU\software\mbox{\sc microsoft\windows\currentversion\sc internet}} \\
  Opens kev:
settings\lockdown_zones\0
   Opens kev:
                                               HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown zones\0
                                               \label{lem:hkcu} \verb+KKCU \software \policies \microsoft \windows \current version \colongorder \part 
   Opens key:
settings\lockdown zones\0
   Opens key:
                                               HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
   Opens kev:
                                              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
   Opens key:
                                               HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown zones\1
   Opens key:
                                               \label{thm:local_continuous} \begin{tabular}{l} HKCU \software \microsoft \windows \current version \since the limit of the local continuous \current version \since the local continuous \since t
settings\lockdown_zones\2
   Opens key:
                                               \label{lem:hklmsoftware policies microsoft windows \current version \ internet \\
settings\lockdown_zones\2
   Opens kev:
                                               HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
                                               HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown zones\3
                                               HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown zones\3
                                               HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\3
   Opens key:
                                               HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
                                               \label{lem:hklmsoftware policies microsoft windows \current version \ internet \\
   Opens key:
settings\lockdown_zones\4
   Opens key:
                                               \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\4
   Opens key:
                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wshtcpip.dll
   Opens key:
                                               HKCU\software\microsoft\internet
explorer \verb|\main| featurecontrol \verb|\feature_disable_legacy_compression| \\
   Opens key:
                                               HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_legacy_compression
   Opens key:
                                               HKLM\software\microsoft\ctf\compatibility\wqwgdy.exe
   Opens key:
HKLM\software\microsoft\windows\currentversion\uninstall\360°Â²Ã^«ÃŽÃ€ÃŠÂ;
                                               HKLM\software\microsoft\windows\currentversion\datetime
   Opens kev:
                                               \label{lem:hklmsoftware} \verb+MKLM+ software+ \verb+microsoft+ windows nt+ current version+ image file execution
   Opens key:
options\wqwgdy.exe\rpcthreadpoolthrottle
   Opens key:
                                               HKLM\system\currentcontrolset\control\securityproviders
   Opens key:
                                               HKLM\system\currentcontrolset\control\lsa\sspicache
   Opens kev:
                                               HKLM\svstem\currentcontrolset\control\lsa\sspicache\msapsspc.dll
                                               HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll
   Opens kev:
                                               HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll
   Opens kev:
   Opens key:
                                               HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
   Opens key:
                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iphlpapi.dll
   Opens key:
                                               HKLM\system\currentcontrolset\services\tcpip\linkage
   Opens key:
                                               HKLM\system\currentcontrolset\services\tcpip\parameters\
   Opens key:
                                               HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
   Opens key:
                                               HKLM\system\currentcontrolset\services\netbt\parameters
   Opens key:
                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msv1_0.dll
   Opens key:
                                               \label{lem:hklmsoftware} \verb+MKLM+ software+ \verb+microsoft+ windows nt+ current version+ image file execution
options\rasadhlp.dll
   Opens key:
                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dnsapi.dll
   Opens key:
                                               HKLM\system\currentcontrolset\services\dnscache\parameters
   Opens key:
                                               HKLM\software\policies\microsoft\windows nt\dnsclient
   Opens key:
                                               HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters
   Opens key
c7d49d7cecdc}
   Opens key:
                                               HKLM\software\policies\microsoft\system\dnsclient
   Opens key:
                                               HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
   Queries value:
                                               HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
   Queries value:
                                               {\tt HKLM \ } system \verb| current control \verb| session manager[safedll sear chmode] \\
   Queries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [transparentenabled]
   Oueries value:
                                               {\tt HKLM \backslash software \backslash microsoft \backslash windows}
nt\currentversion\gre_initialize[disablemetafiles]
   Oueries value:
                                               HKLM\software\microsoft\windows
nt\currentversion\compatibility32[d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174]
   Oueries value:
                                               HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174]
   Queries value:
                                               HKLM\software\microsoft\windows nt\currentversion\windows[appinit dlls]
```

```
Oueries value:
                                                      HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
   Oueries value:
                                                      HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
   Oueries value:
                                                      HKLM\system\setup[systemsetupinprogress]
   Oueries value:
                                                      HKCU\control panel\desktop[multiuilanguageid]
   Queries value:
                                                      HKCU\control panel\desktop[smoothscroll]
   Oueries value:
\label{thm:local_equation} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced[enableballoontips]| \\
   Oueries value:
                                                     {\tt HKLM \ } system \verb|\  current control set \verb|\  control \       | session
manager[criticalsectiontimeout]
                                                      HKLM\software\microsoft\ole[rwlockresourcetimeout]
   Oueries value:
   Oueries value:
                                                      HKCR\interface[interfacehelperdisableall]
                                                      HKCR\interface[interfacehelperdisableallforole32]
   Queries value:
   Queries value:
                                                      HKCR\interface[interfacehelperdisabletypelib]
                                                      HKCR\interface\{00020400-0000-0000-c000-
   Oueries value:
00000000046}[interfacehelperdisableall]
                                                      .
HKCR\interface\{00020400-0000-0000-c000-
   Oueries value:
00000000046} [interfacehelperdisableallforole32]
                                                      ...
HKLM\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[disableimprovedzonecheck]
                                                     HKLM\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_protocol_lockdown[d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exe]
                                                      HKLM\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_protocol_lockdown[*]
                                                      HKLM\software\microsoft\ctf\systemshared[cuas]
   Queries value:
   Queries value:
                                                      HKCU\keyboard layout\toggle[language hotkey]
                                                      HKCU\keyboard layout\toggle[hotkey]
   Queries value:
   Queries value:
                                                      HKCU\keyboard layout\toggle[layout hotkey]
   Queries value:
                                                      HKLM\software\microsoft\ctf[enableanchorcontext]
   Queries value:
                                                      HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
   Oueries value:
                                                      HKCU\software\microsoft\ctf[disable thread input manager]
   Oueries value:
                                                      HKCU\software\microsoft\internet explorer\main[start page]
   Queries value:
                                                      HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
                                                      {\it HKLM} \verb|\system| current controlset| control \verb|\session| \\
   Queries value:
manager\appcompatibility[disableappcompat]
   Queries value:
                                                      HKLM\system\wpa\mediacenter[installed]
    Queries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [authenticode enabled]
                                                      HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
    Queries value:
   Oueries value:
HKLM \ software \ \ icrosoft \ \ is entirely a few and in the limit of the limit 
be2efd2c1a33}[itemdata]
   Queries value:
be2efd2c1a33}[saferflags]
   Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemdata]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[hashalg]
   Oueries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes \setminus \{349d35ab-37b5-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-46666f-9b89-4666
edd5fbde1328}[itemsize]
   Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[saferflags]
   Queries value:
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{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}[itemdata]
   Oueries value:
b813f72dbb91}[hashalg]
   Queries value:
b813f72dbb91}[itemsize]
   Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[saferflags]
   Queries value:
7c29ddecae3f}[itemdata]
7c29ddecae3f}[hashalg]
7c29ddecae3f}[itemsize]
   Queries value:
7c29ddecae3f}[saferflags]
   Oueries value:
085bcc18a68d}[itemdata]
   Queries value:
085bcc18a68d}[hashalg]
   Oueries value:
085bcc18a68d}[itemsize]
   Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
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-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}[hashalg]
  Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemsize]
  Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eh-4fe4-ae2e-
b91490411bfc}[saferflags]
  Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
  Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
                                     HKCU\software\microsoft\windows\currentversion\explorer\shell
  Oueries value:
folders[cache]
  Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
  Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\compatibility32[cmd]
                                     HKLM\software\microsoft\windows nt\currentversion\ime compatibility[cmd]
  Queries value:
                                     HKLM\software\microsoft\command processor[disableunccheck]
  Queries value:
  Oueries value:
                                     HKLM\software\microsoft\command processor[enableextensions]
                                     HKLM\software\microsoft\command processor[delayedexpansion]
  Queries value:
  Queries value:
                                     HKLM\software\microsoft\command processor[defaultcolor]
                                     HKLM\software\microsoft\command processor[completionchar]
  Queries value:
  Queries value:
                                     HKLM\software\microsoft\command processor[pathcompletionchar]
  Queries value:
                                     HKLM\software\microsoft\command processor[autorun]
  Queries value:
                                     HKCU\software\microsoft\command processor[disableunccheck]
  Oueries value:
                                     HKCU\software\microsoft\command processor[enableextensions]
   Oueries value:
                                     HKCU\software\microsoft\command processor[delayedexpansion]
   Queries value:
                                     HKCU\software\microsoft\command processor[defaultcolor]
                                     HKCU\software\microsoft\command processor[completionchar]
   Queries value:
                                     HKCU\software\microsoft\command processor[pathcompletionchar]
   Queries value:
                                     {\tt HKCU \backslash software \backslash microsoft \backslash command \ processor[autorun]}
   Queries value:
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\locale[00000409]
   Queries value:
                                     HKLM \verb|\system| current controlset| control \verb|\nls| language groups[1]
                                     HKLM\software\microsoft\downloadmanager[cacheok]
   Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[createuricachesize]
                                     \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings[createuricachesize]
                                     \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
  Queries value:
settings[enablepunycode]
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
  Queries value:
                                     HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
  Queries value:
                                     HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
  Queries value:
                                     HKLM\software\microsoft\internet
explorer\\ \text{$\text{main}$ feature control$ feature\_mime\_handling[d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exe] }
  Queries value:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[*]
  Oueries value:
                                     HKLM\software\microsoft\ole[maximumallowedallocationsize]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\user agent[]
                                     HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\user agent[]
                                     .
HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\user agent[compatible]
                                     HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\user agent[compatible]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\user agent[version]
                                     HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\user agent[version]
                                     HKCU\software\microsoft\windows\currentversion\internet settings[user
  Queries value:
agent]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Oueries value:
                                     HKLM\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
                                     HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
   Queries value:
ab78-1084642581fb]
                                     HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
   Queries value:
0000-0000000000000]
  Queries value:
                                     \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current \+ version \+ 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]
  Queries value:
                                     \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings[certificaterevocation]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[disablepassport]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
```

```
settings[cachemode]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablebasicoverclearchannel]
 Oueries value:
                           HKCU\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
 Queries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol[feature clientauthcertfilter]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[clientauthbuiltinui]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[sessionstarttimedefaultdeltasecs1
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[signature]
                           \label{local-condition} \verb+HKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings\5.0\cache\content[peruseritem]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\content[peruseritem]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
                           \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current \+ version \+ internet
 Queries value:
settings\5.0\cache\content[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\content[cachelimit]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
 Oueries 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]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
 Oueries value:
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ user shell
folders[history]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings\5.0\cache\history[cacheprefix]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
 Oueries value:
                           HKLM\software\microsoft\rpc[maxrpcsize]
 Oueries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacherepair]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachepath]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cachelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cacheoptions]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cacherepair]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
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]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachepath]
                           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]
                           \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
 Queries value:
settings\5.0\cache\extensible cache\ietld[cacherepair]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
```

```
HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
                                    \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
  Queries value:
settings \verb|\|5.0| cache \verb|\|extensible| cache \verb|\|mshist012014033120140407[ cacheprefix]|
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings \verb|\| 5.0 \verb|\| cache \verb|\| extensible | cache \verb|\| mshist 012014033120140407 [cache limit]|
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
  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]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\privacie:[cacherepair]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\privacie:[cachepath]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\privacie:[cachelimit]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
  Queries value:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[socketreceivebufferlength]
                                    \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current \+ version \+ internet
  Queries value:
settings[keepalivetimeout]
                                    \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
  Queries value:
settings[maxhttpredirects]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[maxconnectionsperserver]
  Queries value:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Queries value:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
                                    HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[connectretries]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[sendtimeout]
  Queries value:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[receivetimeout]
                                    HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[receivetimeout]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[disablentlmpreauth]
  Queries value:
                                    \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current \+ version \+ internet
settings[scavengecachelowerbound]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[certcachenovalidate]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[ftpdefaultexpirytimesecs]
                                    HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exe]
  Queries value:
                                    HKLM\software\microsoft\internet
explorer \verb|\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]|
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
  Oueries value:
                                    \label{thm:local_continuous} \begin{tabular}{l} HKCU \software \microsoft \windows \current version \since the limit of the local continuous \current version \since the local continuous \since t
settings[leashlegacycookies]
```

```
HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablent4rascheck]
 Oueries value:
                      HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
                      \label{lem:hklm} \verb+ Kklm \+ software \+ microsoft \+ windows \+ current version \+ internet
 Queries value:
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]
 Oueries value:
                      HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
 Oueries value:
                      HKLM\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
 Oueries value:
                      HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
                      HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablelegacypreauthasserver]
                      HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablelegacypreauthasserver]
                      HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasshttpnocachecheck]
                      HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasshttpnocachecheck]
                      HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasssslnocachecheck]
                      \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings[bypasssslnocachecheck]
 Oueries value:
                      HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
 Queries value:
                      HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
 Queries value:
                      HKLM\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
 Queries value:
                      HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                      HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dontusednsloadbalancing]
                      \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings[sharecredswithwinhttp]
                      \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
 Queries value:
settings[mimeexclusionlistforcache]
                      HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[headerexclusionlistforcache]
 Queries value:
                      HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
 Queries value:
                      HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
                      HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dnscachetimeout]
 Oueries value:
                      HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
                      HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnalwaysonpost]
                      HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonzonecrossing]
 Oueries value:
                      HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertsending]
                      HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonbadcertrecving]
                      HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonpostredirect]
                      HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[alwaysdrainonredirect]
                      HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonhttpstohttpredirect]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock registry version]
 Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Queries value:
Queries value:
Queries value:
Queries value
Queries value:
Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[packedcatalogitem]
 Oueries value:
                      HKLM\software\microsoft\windows
nt\currentversion\compatibility32[wqwgdy]
 Queries value:
                      HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[wqwgdy]
```

Oueries value: Oueries value: Queries value:

Queries value:

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num] Oueries value:

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

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog \ services \ winsock 2 \ parameters \ names \ pace_catalog \ services \ winsock 2 \ parameters \ names \ pace_catalog \ services \ winsock 2 \ parameters \ names \ pace_catalog \ services \ winsock 2 \ parameters \ names \ pace_catalog \ services \ winsock 2 \ parameters \ names \ pace_catalog \ services \ winsock 2 \ parameters \ names \ pace_catalog \ services \ winsock 2 \ parameters \ names \ pace_catalog \ services \ winsock 2 \ parameters \ names \ pace_catalog \ services \ winsock 2 \ parameters \ names \ pace_catalog \ services \ winsock 2 \ parameters \ names \ pace_catalog \ services \ names \ pace_catalog \ names \ names \ names \ pace_catalog \ names \ names$ Oueries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001fproviderid1 Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog5 \ (catalog_entries \ 00000000001 \ [address family]]$ Queries value:

Oueries value:

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001[version] Oueries value:

Queries value:

Oueries value:

 $HKLM \ system \ current control set \ services \ win sock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 0000000000002 [displaystring]$

Queries value:

Queries value:

 $HKLM \ system \ current control set \ services \ \ winsock 2 \ parameters \ namespace_catalog 5 \ \ catalog_entries \ \ 0000000000002 \ [enabled]$

Queries value:

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 0000000000002 [storesserviceclass info]$ Queries value:

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog \ catalog_entries \ 000000000003 [library path]$ Oueries value:

 $HKLM \ system \ current controls et \ services \ win sock 2 \ parameters \ names pace_catalog5 \ catalog_entries \ 000000000003 \ [displaystring]$ Queries value:

Queries value:

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

Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000003[enabled]

Oueries value: Oueries value:

HKLM\software\microsoft\windows\currentversion\internet

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000003fstoresserviceclassinfol Oueries value:

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

Queries value:

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2 32spincount]

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

settings[globaluseroffline] Queries value:

HKCU\software\microsoft\windows\currentversion\internet

settings[enableautodial] Oueries value:

settings[urlencoding]

Queries value:

HKCU\software\microsoft\windows\currentversion\internet

settings[truncatefilename]

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

settings[badproxvexpirestime]

Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave] HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2] HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3] Queries value: $\label{lem:hklmsoftware} \verb+MKLM\+ software \verb+\microsoft+ windows nt+ current version \verb+\drivers32[wave4]+ \\$ Queries value: Queries value: $HKLM \verb|\software\microsoft\windows| nt\currentversion \verb|\drivers32[wave5]|$ Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8] Queries value: $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 9]$ Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi] Queries value: $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [midi1]$ Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2] Oueries value: $\label{lem:hklmsoftware} \verb+MKLM\+ software \verb+\microsoft+ windows nt+ current version \verb+\drivers32[midi3]$ Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]

HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]

```
Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
  Queries value:
                                   HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [aux 4]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
  Oueries value:
HKLM \label{lem:hklm} Whe all in the label lab
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
  Oueries value:
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
  Queries value:
  Oueries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32maxnumrequestretries]
  Oueries value:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus telephony [tapi32 requestre try time out]
  Queries value:
                                   HKLM\software\microsoft\tracing[enableconsoletracing]
  Queries value:
                                   HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
  Queries value:
                                   HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
  Oueries value:
                                   HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
                                   HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
  Oueries value:
  Queries value:
                                   HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
                                   HKLM\software\microsoft\tracing\rasapi32[filedirectory]
  Queries value:
  Queries value:
                                   HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common appdata]
  Queries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
                                   HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\winlogon[chkaccdebuglevel]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\productoptions[producttype]
  Queries value:
                                   \label{lem:hkcu} \verb+KKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[personal]
  Queries value:
                                   \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ user shell
folders[local settings]
  Queries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\winlogon[rsopdebuglevel]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
  Oueries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\profilelist[profilesdirectory]
  Queries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\profilelist[allusersprofile]
  Oueries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\profilelist[defaultuserprofile]
  Oueries value:
                                   HKLM\software\microsoft\windows\currentversion[programfilesdir]
  Oueries value:
                                   HKLM\software\microsoft\windows\currentversion[commonfilesdir]
                                   HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
  Oueries value:
1757981266-507921405-1957994488-1003[profileimagepath]
                                   HKCU\software\microsoft\windows
  Queries value:
nt\currentversion\winlogon[parseautoexec]
                                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Oueries value:
folders[appdata]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[migrateproxy]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[proxyenable]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[proxyserver]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
  Oueries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
                                   HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_maxconnectionsperserver[d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exe]
                                   HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_maxconnectionsperserver[*]
  Queries value:
                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exe]
  Oueries value:
                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[*]
  Queries value:
                                   HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
  Queries value:
                                   \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings\zones\0[flags]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\zones\2[flags]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\zones\3[flags]
                                   HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
  Oueries value:
```

Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[flags] Oueries value: HKCU\software\microsoft\internet $explorer\\ \\ \text{main}\\ \text{feature}\\ \text{control}\\ \text{feature}\\ \text{local}\\ \text{machine}\\ \text{lockdown}\\ \text{[d488539402abae3873b801373dbc898653f51406ddbd1f32cf3c2fd73a9c3174.exe]}$ Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature localmachine lockdown[*] Queries value: HKLM\software\microsoft\internet Oueries value: HKLM\software\microsoft\internet $\verb|explorer\main\featurecontrol\feature_localmachine_lockdown[*]|$ HKLM\system\currentcontrolset\services\winsock\parameters[transports] Oueries value: Oueries value: ${\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ tcpip \verb|\ parameters \verb|\ winsock[mapping]|$ Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength] Oueries value: HKLM\svstem\currentcontrolset\services\tcpip\parameters\winsock[usedelavedacceptance] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[autodetect] HKLM\software\microsoft\windows\currentversion\datetime[index] Oueries value: HKLM\software\microsoft\rpc\securityservice[10] Queries value: Queries value: HKLM\system\currentcontrolset\control\securityproviders[securityproviders] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name] Queries value: Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type] Queries value: Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize] HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid] Queries value: Queries value: Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type] Oueries value: Oueries value: Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment] Queries value: $HKLM \verb|\system| current controlset \verb|\control| lsa \verb|\sspicache| msnsspc.dll[rpcid]|$ Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version] Oueries value: Oueries value: Oueries value: $HKLM \setminus system \setminus current control \\ \ \mid sa \setminus spicache \setminus msnsspc.dll[tokensize]$ HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll] Oueries value: HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\3[1a10] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[quervadaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Queries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Queries value: $\label{lem:hklm} \verb+Kklm \system \current control set \services \$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Queries value: $\label{lem:hklm} \verb|HKLM| system| current control set | services| dns cache | parameters [wait for name error on all]| | for the parameters | for the param$ $\label{lem:hklmsystem} \\ \text{HKLM} \\ \text{system} \\ \text{currentcontrolset} \\ \text{services} \\ \text{dnscache} \\ \text{parameters} \\ \text{[useedns]} \\ \\ \text{parameters} \\ \text{[useedns]} \\ \text{parameters} \\ \text{[useedns]} \\ \text{parameters} \\ \text{[useedns]} \\ \text{parameters} \\ \text{[useedns]} \\ \text{[u$ Queries value: Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [queryipm atching]$ Oueries value: $HKLM \verb|\system| current controlset \verb|\services| dns cache \verb|\parameters[use hostsfile]|$

HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]

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

Oueries value:

Oueries value:

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Queries value: Queries value: Oueries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[registerwanadapters] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [disable wandynamic update]$ Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Queries value: Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Oueries value: $\label{lem:hklm} \verb+Kklm \system \current control set \services \label{lem:hklm} \verb+ dn scache \parameters [server prior ity time limit]$ Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [maxcached sockets]$ Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [dnsquery time outs]$ Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [dnsquick query time outs]$ Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts] HKLM\svstem\currentcontrolset\services\tcpip\linkage[bind] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[enabledhcp] Queries value: c7d49d7cecdc}[leaseobtainedtime] Oueries value: c7d49d7cecdc}[leaseterminatestime] Queries value: c7d49d7cecdc}[dhcpserver] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain] Oueries value: c7d49d7cecdc}[queryadaptername] Queries value: c7d49d7cecdc}[disableadapterdomainname] Queries value: c7d49d7cecdc}[registrationenabled] Queries value: c7d49d7cecdc}[registeradaptername] Oueries value: c7d49d7cecdc}[registrationmaxaddresscount] Queries value: c7d49d7cecdc}[maxnumberofaddressestoregister] Queries value: $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-a$ c7d49d7cecdc}[domain] Oueries value: c7d49d7cecdc}[dhcpdomain]

Oueries value:

c7d49d7cecdc}[ipautoconfigurationenabled] Oueries value: $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-a$ c7d49d7cecdc}[addresstype] Queries value: c7d49d7cecdc}[nameserver] Oueries value: c7d49d7cecdc}[dhcpnameserver] HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist] Oueries value: Queries value: $\label{lem:hklm} \verb+Kklm \ system \ current control set \ \verb+services \ \verb+tcpip \ parameters [dnsnbtlookuporder]$ HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong Oueries value: cryptographic provider[type] HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong Oueries value: cryptographic provider[image path] HKLM\software\microsoft\windows\currentversion\datetime[index] Sets/Creates value: Sets/Creates value: HKLM\software\microsoft\windows\currentversion\datetime[sid] HKLM\software\microsoft\cryptography\rng[seed] Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell Value changes: folders[cache] Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cookies] Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[history] Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell folders[common appdata] Value changes: $\label{thm:linear} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\shell}} \\$ folders[appdata]

Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\connections[savedlegacysettings]

Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\rongman[nrovybyass]

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