Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3327, Task ID: 816

Task ID: 816 Risk Level: 10

Date Processed: 2016-05-18 10:41:41 (UTC)

Processing Time: 7.76 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\6f2064e626e4383a5d8a9c0bdb8e9ddf.exe"

Sample ID: Type: basic admin Owner:

6f2064e626e4383a5d8a9c0bdb8e9ddf Label:

Date Added: 2016-05-18 10:30:51 (UTC) PE32:win32:gui File Type:

File Size: 118784 bytes

6f2064e626e4383a5d8a9c0bdb8e9ddf MD5:

d0fae395b7a83a222a795282e88c1d87ca83c3499a2a343f607b8e6c5832cd27 SHA256:

Description: None

Pattern Matching Results

3 HTTP connection - response code 200 (success)

3 Long sleep detected

4 Terminates process under Windows subfolder

10 Creates malicious events: Beebone [Trojan]

6 Checks task list from command line

Process/Thread Events

C:\WINDOWS\Temp\6f2064e626e4383a5d8a9c0bdb8e9ddf.exe Creates process:

"c:\windows\temp\6f2064e626e4383a5d8a9c0bdb8e9ddf.exe"]
Creates process: C:\WINDOWS\system32\cmd.exe ["C:\WINDOWS\system32\cmd.exe" /c

tasklist&&del 6f2064e626e4383a]

Creates process: C:\WINDOWS\system32\tasklist.exe [tasklist]

RASMAN [C:\WINDOWS\system32\svchost.exe -k netsvcs] Loads service: Terminates process: C:\WINDOWS\Temp\6f2064e626e4383a5d8a9c0bdb8e9ddf.exe

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

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 Creates mutex:

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

Creates mutex:

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

507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003

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

settings!temporary internet files!content.ie5!

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

settings!history!history.ie5!

\BaseNamedObjects\WininetConnectionMutex Creates mutex: Creates mutex:

\BaseNamedObjects\ZonesCounterMutex Creates mutex:

\BaseNamedObjects\ZoneAttributeCacheCounterMutex \BaseNamedObjects\ZonesCacheCounterMutex Creates mutex: Creates mutex: $\verb|\BaseNamedObjects\ZonesLockedCacheCounterMutex| \\$

\BaseNamedObjects\SHIMLIB_LOG_MUTEX Creates mutex:

\BaseNamedObjects\userenv: User Profile setup event Creates event: \BaseNamedObjects\C:?WINDOWS?TEMP?6F2064E626E4383A5D8A9C0BDB8E9DDF.EXE Creates semaphore:

Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1} \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D} Creates semaphore: Creates semaphore: \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}

File System Events

Creates C:\Documents and Settings\Admin\Cookies\admin@domai.noip1[1].txt C:\WINDOWS\Prefetch\6F2064E626E4383A5D8A9C0BDB8E9-2D1CD2A3.pf Opens: Opens: C:\Documents and Settings\Admin

Opens: C:\WINDOWS\system32\msvbvm60.dll C:\WINDOWS\system32\imm32.dll Opens: Opens: C:\WINDOWS\system32\rpcss.dll Opens: C:\WINDOWS\system32\MSCTF.dll Opens: C:\WINDOWS\system32\sxs.dll

```
C:\WINDOWS\system32\MSCTFIME.IME
 Opens:
                         C:\WINDOWS\system32\winmm.dll
 Opens:
                         {\tt C:\WINDOWS\Temp\6f2064e626e4383a5d8a9c0bdb8e9ddf.exe}
 Opens:
 Opens:
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Config
                         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
                         C:\WINDOWS\WindowsShell.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\WindowsShell.Config
 Opens:
                         C:\WINDOWS\system32\wininet.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\wininet.dll.123.Config
 Opens:
                         C:\WINDOWS\system32\shell32.dll
                         C:\WINDOWS\system32\SHELL32.dll.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Config
 Opens:
                         C:\WINDOWS\system32\comctl32.dll
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Config
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History\History.IE5
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Cookies
 Opens:
                         C:\Documents and Settings\Admin\Cookies\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\index.dat
                         C:\WINDOWS\system32\ws2_32.dl1
 Opens:
 Opens:
                         C:\WINDOWS\system32\ws2help.dll
 Opens:
                         C:\WINDOWS\system32\rasapi32.dll
 Opens:
                         C:\WINDOWS\system32\rasman.dll
 Opens:
                         C:\WINDOWS\system32\netapi32.dll
 Opens:
                         C:\WINDOWS\system32\tapi32.dll
 Opens:
                         C:\WINDOWS\system32\rtutils.dll
 Opens:
                         C:\WINDOWS\system32\TAPI32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\TAPI32.dll.124.Config
                         C:\AUTOEXEC.BAT
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Application
Data\Microsoft\Network\Connections\Pbk
 Opens:
                         C:\WINDOWS\system32\ras
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\Network\Connections\Pbk\
                         C:\WINDOWS\system32\sensapi.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\mswsock.dll
 Opens:
                         C:\WINDOWS\system32\rasadhlp.dll
 Opens:
                         C:\WINDOWS\system32\msv1_0.dll
 Opens:
                         C:\WINDOWS\system32\iphlpapi.dll
 Opens:
                         C:\WINDOWS\system32\dnsapi.dll
 Opens:
                         C:\WINDOWS\system32\drivers\etc\hosts
 Opens:
                         C:\WINDOWS\system32\rsaenh.dll
 Opens:
                         C:\WINDOWS\system32\crypt32.dll
 Opens:
                         C:\WINDOWS\system32\hnetcfg.dll
 Opens:
                         C:\WINDOWS\system32\wshtcpip.dll
 Opens:
                         C:\Documents and Settings\Admin\Cookies\admin@domai.noip1[1].txt
                         C:\WINDOWS\system32\ieframe.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\clbcatq.dll
 Opens:
                         C:\WINDOWS\system32\comres.dll
                         {\tt C:\WINDOWS\Registration\R0000000000007.clb}
 Opens:
 Opens:
                         C:\Program Files\Internet Explorer\iexplore.exe
 Opens:
                         C:\WINDOWS\system32\ieframe.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\ieframe.dll.123.Config
 Opens:
                         C:\WINDOWS\system32\en-US\ieframe.dll.mui
 Opens:
                         C:\WINDOWS\system32
                         C:\WINDOWS
 Opens:
 Opens:
                         C:\WINDOWS\system32\setupapi.dll
 Opens:
                         C:\WINDOWS\system32\cmd.exe
                         {\tt C:\WINDOWS\AppPatch\symmin.sdb}
 Opens:
 Opens:
                         C:\WINDOWS\AppPatch\systest.sdb
                         C:\WINDOWS\system32\cmd.exe.Manifest
 Opens:
                         C:\WINDOWS\WINHELP.INI
 Opens:
 Opens:
                         C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf
 Opens:
                         C:
                         C:\WINDOWS\AppPatch
 Opens:
 Opens:
                         C:\WINDOWS\system32\wbem
 Opens:
                         C:\WINDOWS\WinSxS
                         C:\WINDOWS\system32\ntdll.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\kernel32.dll
 Opens:
                         C:\WINDOWS\svstem32\unicode.nls
 Opens:
                         C:\WINDOWS\system32\locale.nls
```

C:\WINDOWS\system32\sorttbls.nls Opens: Opens: C:\WINDOWS\system32\msvcrt.dll C:\WINDOWS\system32\user32.dll Opens: Opens: C:\WINDOWS\system32\gdi32.dll Opens: C:\WINDOWS\system32\shimeng.dll C:\WINDOWS\AppPatch\AcGenral.dll Opens: Opens: C:\WINDOWS\system32\advapi32.dll C:\WINDOWS\system32\rpcrt4.dll Opens: C:\WINDOWS\system32\secur32.dll Opens: 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 Opens: C:\WINDOWS\system32\userenv.dll C:\WINDOWS\system32\uxtheme.dll Opens: Opens: C:\WINDOWS\system32\ctype.nls Opens: C:\WINDOWS\system32\sortkey.nls Opens: C:\WINDOWS\system32\apphelp.dll Opens: C:\WINDOWS\system32\wbem\wmic.exe Opens: C:\Documents and Settings Opens: C:\WINDOWS\system32\tasklist.exe

Opens: C:\WINDOWS\system32\tasklist.exe.Manifest
Opens: C:\WINDOWS\Prefetch\TASKLIST.EXE-10D94B23.pf
Opens: C:\WINDOWS\system32\wbem\framedyn.dll

C:\WINDOWS\system32\dbghelp.dll Opens: Opens: C:\WINDOWS\system32\winlogon.exe Opens: C:\WINDOWS\system32\xpsp2res.dll C:\WINDOWS\system32\wbem\wbemprox.dll Opens: Opens: C:\WINDOWS\system32\wbem\wbemcomn.dll Opens: C:\WINDOWS\system32\winsta.dll Opens: C:\WINDOWS\system32\wbem\wbemsvc.dll Opens: C:\WINDOWS\system32\wbem\fastprox.dll Opens: C:\WINDOWS\system32\msvcp60.dll Opens: C:\WINDOWS\system32\ntdsapi.dll

Writes to: C:\Documents and Settings\Admin\Cookies\admin@domai.noip1[1].txt

Reads from: C:\WINDOWS\Temp\6f2064e626e4383a5d8a9c0bdb8e9ddf.exe

Reads from: C:\AUT0EXEC.BAT

Reads from: C:\WINDOWS\system32\drivers\etc\hosts
Reads from: C:\WINDOWS\system32\rsaenh.dll
Reads from: C:\WINDOWS\Registration\R000000000007.clb

Reads from: C:\WINDOWS\system32\cmd.exe

Reads from: C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf

Network Events

DNS query: domai.noip1.org

DNS response: $domai.noip1.org \Rightarrow 69.195.129.70$

Connects to: 69.195.129.70:443

Sends data to: 8.8.8.8:53

Sends data to: domai.noip1.org:443 (69.195.129.70)

Receives data from: 0.0.0.0:0

Receives data from: domai.noip1.org:443 (69.195.129.70)

Windows Registry Events

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

folders

 $\label{lem:creates} \mbox{Creates key:} \qquad \mbox{HKCU\software\mbox{\sm microsoft\windows\currentversion\explorer\sm hell folders} \\$

Creates key: HKLM\software\microsoft\tracing

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

folders

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

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

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

settings\connections

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

awareness Creates ke

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

settings\p3p\history

 $\label{lem:condition} {\it Creates key:} \qquad \qquad {\it HKCU\software\microsoft\windows\currentversion\explorer}$

Creates key:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current \vee explorer \setminus session in fo \setminus 000000000000000352$

Creates key: HKLM\software\microsoft\windows\currentversion\shell extensions\blocked Creates key: HKCU\software\microsoft\windows\currentversion\shell extensions\blocked Creates key: HKLM\software\microsoft\windows\currentversion\shell extensions\cached HKCU\software\microsoft\windows\currentversion\shell extensions\cached Creates key: HKCU\software\microsoft\windows\currentversion\shell extensions\cached

Creates key:

806d6172696f}\

Creates key: HKCU\software\microsoft\visual basic\6.0

Creates key: HKCU\software

Creates key: HKCU\software\microsoft

Creates key: HKCU\software\microsoft\visual basic
Creates key: HKCU\software\microsoft\multimedia\audio

Creates key: HKCU\software\microsoft\multimedia\audio compression manager\
Creates key: HKCU\software\microsoft\multimedia\audio compression manager\msacm
Creates key: HKCU\software\microsoft\multimedia\audio compression manager\priority

v4.00

Creates kev: HKLM\software\microsoft\wbem\cimom

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

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

options\6f2064e626e4383a5d8a9c0bdb8e9ddf.exe

Opens key: HKLM\system\currentcontrol\set\control\terminal server
Opens key: HKLM\system\currentcontrol\set\control\safeboot\option

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\gdi32.dll

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

options\user32.dll

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

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

options\imm32.dll

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

options\ntdll.dll

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

options\kernel32.dll

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

options\secur32.dll

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

options\rpcrt4.dll

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

options\advapi32.dll

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

options\msvcrt.dll

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

options\ole32.dll

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

options\oleaut32.dll

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

 $options \verb|\msvbvm60.dll|$

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

Opens key: $\begin{tabular}{ll} HKLM\software\microsoft\windows nt\currentversion\winlogon \\ Opens key: \\ \begin{tabular}{ll} HKLM\end{tabular} \label{eq:hklm}$

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

Opens key: HKLM\software\microsoft\ole

Opens key: HKCR\interface

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

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

Opens key: HKCU\

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

Opens key: HKCU\control panel\desktop

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

options\msctf.dll

Opens key:

HKLM\software\microsoft\ctf\compatibility\6f2064e626e4383a5d8a9c0bdb8e9ddf.exe

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

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

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

options\sxs.dll

Opens key: HKLM\system\setup

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

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

options\version.dll

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

options\msctfime.ime

Opens key: HKCU\software\microsoft\ctf

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

Opens key: HKLM\system\currentcontrolset\control\nls\codepage

Opens key: HKLM\software\microsoft\vba\monitors

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

options\winmm.dll

HKLM\software\microsoft\windows nt\currentversion\drivers32 Opens kev:

Opens key:

HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm

Opens kev: HKLM\system\currentcontrolset\services\disk\enum

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

options\shlwapi.dll

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

options\normaliz.dll

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

options\iertutil.dll

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

options\urlmon.dll

Opens key:

HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots

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

options\comctl32.dll

Opens key: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\advanced}} \\$ Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\lz32.dll

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

options\wininet.dll

Opens key: HKCU\software\classes\

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

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

settings

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

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\

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

Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol 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: $\label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ settings\zonemap\domains\

Opens key:

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

settings\zonemap\domains\ Opens kev:

HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\

 $\label{lem:hkcu} \verb+KCU\software\policies\microsoft\windows\currentversion\currenters$ 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: HKLM\system\currentcontrolset\control\wmi\security

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

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

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

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

settings\5.0\cache

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

settings\5.0\cache\content

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

settings\5.0\cache\content

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

options\shell32.dll

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
 Opens kev:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\6f2064e626e4383a5d8a9c0bdb8e9ddf.exe\rpcthreadpoolthrottle
 Opens key:
                         HKLM\software\policies\microsoft\windows nt\rpc
                         HKLM\system\currentcontrolset\control\computername
 Opens key:
 Opens key:
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
```

HKLM\system\currentcontrolset\control\computername\activecomputername

settings\5.0\cache\extensible cache

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

settings\5.0\cache\extensible cache\domstore

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

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

settings\5.0\cache\extensible cache\iecompat

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

settings\5.0\cache\extensible cache\ietld

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

settings\5.0\cache\extensible cache\mshist012014033120140407

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

settings\5.0\cache\extensible cache\mshist012014041220140413

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

settings\5.0\cache\extensible cache\privacie:

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset

HKLM\software\microsoft\internet Opens key:

explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_bufferbreaking_818408 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_bufferbreaking_818408 Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954

HKLM\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954

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

settings\5.0\cache

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

settings\5.0\cache

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289

HKLM\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled $\label{local-objective} \verb|HKCU| software \verb|microsoft| internet| \\$ Opens key:

explorer\main\featurecontrol\feature_allow_long_international_filenames

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_allow_long_international_filenames

HKCU\software\microsoft\internet Opens key:

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 key:

explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback HKLM\software\microsoft\internet Opens kev:

explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback

HKCU\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_disallow_null_in_response_headers

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_disallow_null_in_response_headers

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

HKLM\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature digest no extras in uri Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059

Opens kev: HKLM\software\microsoft\internet

explorer\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 kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000003 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004 Opens key: Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007 Opens key: Opens key: Opens key: $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ (catalog_entries \ 000000000010) \ (catalog_entries \ (catalog \ (catalog_entries \ (catalog \ (catal$ Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000011 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004 Opens key: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog5 \ catalog_entries$ HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001 Opens key: Opens key: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\wpad}} \\$ 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: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_http_username_password_disable HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_http_username_password_disable Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\netapi32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasman.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rtutils.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\tapi32.dll Opens key: HKLM\software\microsoft\windows\currentversion\telephony Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasapi32.dll Opens key: HKLM\software\microsoft\tracing\rasapi32 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\userenv.dll Opens key: HKLM\system\currentcontrolset\control\productoptions Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders ${\tt HKLM \backslash software \backslash policies \backslash microsoft \backslash windows \backslash system}$ Opens key: Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ profile list$ Opens kev: HKLM\system\currentcontrolset\control\session manager\environment Opens key: HKLM\software\microsoft\windows\currentversion Opens key: HKU\ Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003 Opens key: HKCU\environment Opens kev: HKCU\volatile environment Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\sensapi.dll

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

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

filters\rpa
 Opens key:
filters\rpa

Opens kev:

Opens key: HKCU\software\microsoft\internet

```
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
                         HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_mime_handling
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\mswsock.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasadhlp.dll
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\protocoldefaults\
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
                         HKLM\software\microsoft\windows\currentversion\internet
 Opens key:
settings\zonemap\domains\msn.com
                         HKLM\software\microsoft\windows\currentversion\internet
 Opens key:
settings\zonemap\domains\msn.com\related
 Opens key:
                         HKLM\software\microsoft\rpc\securityservice
 Opens key:
                         HKLM\system\currentcontrolset\control\securityproviders
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
 Opens key:
                         HKCU\software\microsoft\internet explorer\ietld
 Opens key:
                         HKLM\software\policies\microsoft\internet explorer\security
                         HKLM\system\currentcontrolset\control\lsa\sspicache
 Opens key:
 Opens key:
                         HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.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 \setminus software \setminus microsoft \setminus windows \setminus current version \setminus internet settings \setminus zones \setminus 1
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
                         HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
 Opens key:
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
 Opens key:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\
 Opens key:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
                         Opens key:
 Opens key:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\0
                         HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll
 Opens kev:
 Opens key:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\1
 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\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
 Opens key:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
                         HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\3
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\zones\3
 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:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
 Opens key:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
 Opens key:
                         HKLM\software\microsoft\internet
```

```
explorer\main\featurecontrol\feature_localmachine_lockdown
                                                HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\
   Opens key:
                                                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
   Opens key:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                                                HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\0
   Opens key:
                                                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
   Opens key:
                                                \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
settings\lockdown_zones\0
   Opens key:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
   Opens key:
                                                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
   Opens key:
                                                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                                                HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\2
                                                HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\2
   Opens key:
                                                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
                                                HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\3
                                                HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\3
   Opens key:
                                                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                                                HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\4
   Opens key:
                                                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
                                                HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\4
   Opens key:
                                                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
   Opens key:
                                                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
options\dnsapi.dll
                                                \label{lem:hklm} \verb+Kklm \system \current control set \services \
   Opens key:
   Opens key:
                                                HKLM\software\policies\microsoft\windows nt\dnsclient
   Opens key:
                                                HKLM\system\currentcontrolset\services\tcpip\parameters
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}
   Opens key:
                                                HKLM\software\policies\microsoft\system\dnsclient
                                                HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
   Opens key:
cryptographic provider
   Opens key:
                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rsaenh.dll
                                                HKLM\software\policies\microsoft\cryptography
   Opens kev:
   Opens key:
                                                HKLM\software\microsoft\cryptography
   Opens key:
                                                HKLM\software\microsoft\cryptography\offload
   Opens key:
                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\hnetcfg.dll
   Opens key:
                                                HKLM\system\currentcontrolset\services\winsock\parameters
   Opens key:
                                                HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
   Opens key:
                                                \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution
options\wshtcpip.dll
                                                HKCU\software\microsoft\internet explorer\ietld\lowmic
   Opens kev:
   Opens key:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings\p3p\history\noip1.org
   Opens key:
HKLM \ software \ `microsoft \ 'windows \ 'current version' shell compatibility \ 'applications' \ '6f2064e626e4383a5d8a9c0bdb8e9ddf. exemple in the compatibility in the compa
   Opens key:
                                                HKCU\software\microsoft\windows\currentversion\explorer
   Opens kev:
                                                HKLM\software\microsoft\windows\currentversion\explorer
   Opens key:
                                                HKLM\software\microsoft\windows\currentversion\policies\explorer
                                                \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+policies \verb+explorer+ \\
   Opens kev:
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace
   Opens key:
bc06-4ada335c892b}
ba4f-00a0c91eedba}
   Opens key:
98a8-0800361b1103}
```

Opens key:

9f08-00aa002f954e}

Onens key

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ desktop \ names pace \ \{e17d4fc0-5564-11d1-e17d4fc0-5564$

83f2-00a0c90dc849}

Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\desktop\namespace

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

Opens key:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current \lor explorer \setminus session in follow 000000000000352 \setminus desktop \setminus names pace the following of the f$

Opens key: HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder

Opens key: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder

Opens key: HKCU\software\classes\clsid\{208d2c60-3aea-1069-a2d7-

08002b30309d}\shellfolder

Opens key: HKCR\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder

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

08002b30309d}\shellfolder

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

Opens key:

HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{871c5380-42a0-1069-

a2ea-08002b30309d}

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

08002b30309d}\inprocserver32

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\apphelp.dll

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

Opens key: HKLM\software\microsoft\com3

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

options\comres.dll

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

options\clbcatq.dll

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

Opens key: HKLM\software\classes

Opens key: HKCR\clsid

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

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

08002b30309d}\treatas

08002b30309d}\inprocserverx86

 $Opens~key: \\ HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\ \ inprocserverx86 \\$

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

 $08002b30309d \} \\ local server 32$

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

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

08002b30309d}\inprochandler32

 $Opens~key: \\ HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\ \ inprochandler 32 \\$

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

 $08002b30309d \verb|\inprochandlerx86|$

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

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

08002b30309d}\localserver

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

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

options\ieframe.dll

Opens key: HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe

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

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

0000c05bae0b}\typelib

Opens key: $HKCR \cdot \{-ab22ac1-30c1-11cf-a7eb-0000c05bae0b\} \cdot \{-ab22ac1-30c1-11$

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

Opens key: HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32

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

 ${\tt 00aa004ba90b} \verb|\proxystubclsid32| \\$

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

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

00000000046}\proxystubclsid32

Opens key: HKCR\interface\{000214e6-0000-0000-c000-0000000046}\proxystubclsid32

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

00c04f79abd1}\proxystubclsid32

Opens key: HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32

Opens key: HKCU\software\classes\clsid\{11016101-e366-4d22-bc06-

4ada335c892b}\shellfolder

Opens key: HKCR\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder

Opens key: HKCU\software\classes\clsid\{1f4de370-d627-11d1-ba4f-

00a0c91eedba}\shellfolder

```
HKCR \c1sid \f1f4de370-d627-11d1-ba4f-00a0c91eedba \c1sid \c1si
Opens key:
Opens key:
                                                                                                                                                                                                                                                                                                                                                                                  HKCU\software\classes\clsid\{450d8fba-ad25-11d0-98a8-
```

0800361b1103}\shellfolder

HKCR\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder Opens key:

Opens kev: HKCU\software\classes\clsid\{645ff040-5081-101b-9f08-

00aa002f954e}\shellfolder

Opens key: HKCU\software\classes\clsid\{e17d4fc0-5564-11d1-83f2-Opens key:

00a0c90dc849}\shellfolder

HKCR\clsid\{e17d4fc0-5564-11d1-83f2-00a0c90dc849}\shellfolder Opens key:

Opens kev:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus shell execute hooks$ Opens key: HKCU\software\classes\clsid\{aeb6717e-7e19-11d0-97ee-

00c04fd91972}\inprocserver32

Opens key: $HKCR\clsid\\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\\{inprocserver32}$ Opens key: HKLM\software\microsoft\windows\currentversion\app paths\cmd.exe HKLM\software\microsoft\windows\currentversion\policies\associations Opens kev: Opens key: HKCU\software\microsoft\windows\currentversion\policies\associations

Opens key: HKCU\software\classes\.exe

Opens key: HKCR\.exe

Opens key: HKCU\software\classes\.ade

Opens key: HKCR\.ade

HKCU\software\classes\.adp Opens kev:

Opens key: HKCR\.adp

Opens key: HKCU\software\classes\.app

Opens key: HKCR\.app

Opens key: HKCU\software\classes\.asp

Opens key: HKCR\.asp

HKCU\software\classes\.bas Opens key:

Opens key: HKCR\.bas

Opens key: HKCU\software\classes\.bat

Opens key: HKCR\.bat

Opens key: HKCU\software\classes\.cer

Opens key: HKCR\.cer

HKCU\software\classes\.chm Opens key:

Opens key: HKCR\.chm

Opens key: HKCU\software\classes\.cmd

Opens key: HKCR\.cmd

Opens key: HKCU\software\classes\.com

Opens key: HKCR\.com

Opens key: HKCU\software\classes\.cpl

Opens key: HKCR\.cpl

HKCU\software\classes\.crt Opens kev: HKCR\.crt

Opens key:

Opens key: HKCU\software\classes\.csh

Opens key: HKCR\.csh

Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4\}$

Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4} HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-Opens kev:

00c04fb6bfc4}\treatas

HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-Opens key:

00c04fb6bfc4}\inprocserver32

HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32 Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-Opens kev:

00c04fb6bfc4}\inprocserverx86

 $HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserverx86$ Opens key:

HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-Opens key:

00c04fb6bfc4}\localserver32

 $HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver32$ Opens key:

Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4\inprochandler32

 $HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\clsid$ Opens key:

HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-Opens kev:

00c04fb6bfc4}\inprochandlerx86

HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandlerx86 Opens kev:

Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\localserver

Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver

Opens kev: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610

Opens kev: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000

HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{20d04fe0-3aea-1069-

a2d8-08002b30309d}

Opens key: HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\inprocserver32

Opens key: $HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32$ Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\setupapi.dll

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

Opens key: HKLM\system\wpa\pnp

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

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

Opens key:

 $\label{thm:linear} \mbox{HKCU\software\mbox{\sc windows\currentversion\explorer\mbox{\sc windows\currentversion\explorer\sc windows\currentversion\explorer\sc windows\currentversion\explorer\sc windows\currentversion\explorer\sc windows\currentversion\explorer\sc windows\currentversion\explorer\sc windows\currentversion\explorer\sc windows\currentversion\explorer\sc windows\currentversion\explorer\sc windows\currentversion\explorer\explor$

Opens key:

11e3-9fc7-806d6172696f}\

Opens key: HKCU\software\classes\drive\shellex\folderextensions

Opens key: HKCR\drive\shellex\folderextensions

Opens key: HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-

4442-804e-409d6c4515e9}

Opens key: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-

409d6c4515e9}

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

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

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

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

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

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

Opens key: HKCR\directory\clsid

Opens key: HKCU\software\classes\folder

HKCR\folder Opens key:

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

Opens key: HKCR\folder\clsid

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

Opens key: HKCU\software\classes\exefile

HKCR\exefile Opens key:

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

Opens key: HKCR\exefile\curver

HKCR\exefile\ Opens key:

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

Opens key: HKCR\exefile\shellex\iconhandler

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

Opens key: HKCR\systemfileassociations\.exe

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

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

Opens key: HKCR\exefile\clsid HKCU\software\classes* Opens key:

Opens key: HKCR*

HKCU\software\classes*\clsid Opens kev:

HKCR*\clsid Opens key:

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

Opens key: HKCR\exefile\shell

Opens key: HKCU\software\classes\exefile\shell\open

Opens key: HKCR\exefile\shell\open

Opens kev: HKCU\software\classes\exefile\shell\open\command

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

Opens kev:

HKCU\software\microsoft\windows\currentversion\policies\explorer\restrictrun HKCU\software\classes\exefile\shell\open\ddeexec Opens key:

Opens key: HKCR\exefile\shell\open\ddeexec

Opens key: HKCU\software\classes\applications\cmd.exe

Opens key: HKCR\applications\cmd.exe

Opens key: HKCU\software\microsoft\windows\shellnoroam

Opens key: HKCU\software\microsoft\windows\shellnoroam\muicache HKCU\software\microsoft\windows\shellnoroam\muicache\ Opens key:

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

Opens key: HKLM\system\wpa\tabletpc Opens key: HKLM\system\wpa\mediacenter

Opens key: $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} in the constant of the constan$

Opens key: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags\custom\cmd.exe

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags Opens key: HKLM\software\policies\microsoft\windows\safer\levelobjects

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

Opens kev:

be2efd2c1a33}

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

Opens key:

edd5fbde1328}

Opens key:

```
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb913
  Opens key:
7c29ddecae3f}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc3
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
  Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus paths
  Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
  Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus hashes
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
                            HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus paths
  Opens key:
                            HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
  Opens key:
  Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
  Opens key:
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 kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
  Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
                            HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Opens kev:
                            HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\cmd.exe
  Opens key:
                            HKLM\software\microsoft\windows
                            HKLM\software\microsoft\windows\html help
  Opens kev:
                            HKLM\software\microsoft\windows\help
```

Opens key:

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

options\acgenral.dll

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

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

options\msacm32.dll

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

options\uxtheme.dll

Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache

Opens key:

 $HKLM \verb|\software\m| icrosoft\audiocompression manager\driver cache\m| sacm.imaadpcm$

Opens key:

Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711

Opens key:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610

Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723

Opens key:

 $HKLM \ \ software \ \ \ microsoft \ \ \ audio compression manager \ \ \ \ msaudio 1$

Opens key:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet

Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.13acm

Opens key: HKLM\system\currentcontrolset\control\mediaresources\acm
Opens key: HKCU\software\microsoft\windows\currentversion\thememanager

Opens key: HKCU\software\policies\microsoft\windows\system
Opens key: HKLM\software\microsoft\command processor
Opens key: HKCU\software\microsoft\command processor
Opens key: HKLM\system\currentcontrol\set\control\nls\locale

 $Opens\;key: \\ \qquad \qquad \text{HKLM} system \verb|\currentcontrolset| control| nls \verb|\locale| alternate sorts| \\$

Opens key: HKLM\system\currentcontrolset\control\nls\language groups

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\tasklist.exe

Opens key: ${\tt HKLM} \verb| software \verb| micros of t \verb| windows nt \verb| current version \verb| time secution | time secu$

options\tasklist.exe

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

options\mpr.dll

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

options\framedyn.dll
Opens kev:

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

options\dbghelp.dll

Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder

Opens key: HKLM\software\microsoft\wbem\cimom

Opens key: HKLM\software\microsoft\ctf\compatibility\tasklist.exe

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

 $options \verb|\tasklist.exe| rpcthreadpoolthrottle$

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

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

options\xpsp2res.dll

Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}

Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-

 $00aa004b2e24 \} \verb|\treatas|$

 $\label{lem:continuous} Opens \ key: \\ Opens \ key: \\ HKCQ \ Software \ classes \ clsid \ \{4590f811-1d3a-11d0-891f-00aa004b2e24\} \ treatas \\ Opens \ key: \\ HKCU \ Software \ classes \ clsid \ \{4590f811-1d3a-11d0-891f-00aa004b2e24\} \ treatas \\ Opens \ key: \\ Op$

 $00aa004b2e24 \} \verb|\inprocserver32|$

Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\inprocserverx86

Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\localserver32

 $Opens~key: \\ HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\localserver 32$

Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\inprochandler32

Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler32

Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\inprochandlerx86

 $Opens~key: \\ HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\ \ inprochandler x86 \\$

Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\localserver

Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\localserver

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

options\wbemcomn.dll

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

options\wbemprox.dll

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

options\winsta.dll

 $Opens~key: \\ HKCU \setminus software \\ \\ classes \\ \\ clsid \\ \\ \{8bc3f05e-d86b-11d0-a075-00c04fb68820\} \\ \\$

Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\treatas

00c04fb68820}\inprocserver32

Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserver32

Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprocserverx86

Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserverx86

Opens key: $\label{localization} \mbox{HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-d86$

00c04fb68820}\localserver32

Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver32

Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

 ${\tt 00c04fb68820} \verb|\inprochandler32|$

 $\label{locality} $$HKCR\clsid{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandler 32$$ Opens key:

Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprochandlerx86

HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandlerx86 Opens key:

Opens kev: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\localserver

 $HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820\}\localserver$ Opens key: HKCU\software\classes\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820} Opens key:

Opens key: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}

HKCU\software\classes\interface\{f309ad18-d86a-11d0-a075-00c04fb68820} Opens key:

Opens key: HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820} Opens key: $HKCU \setminus software \setminus classes \setminus interface \setminus \{f309ad18 - d86a - 11d0 - a075 - d86a - 11d0 - a075 - d86a - d86a$

00c04fb68820}\proxystubclsid32

Opens key: Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}

HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24} Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-Opens kev:

00aa004b2e24}\treatas

Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\treatas Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{7c857801-7381-11cf-884d-11cf-885d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11c$

00aa004b2e24}\inprocserver32

Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32

HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-Opens kev:

00aa004b2e24}\inprocserverx86

Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-

00aa004b2e24}\localserver32

Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\localserver32

HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-Opens kev:

00aa004b2e24}\inprochandler32

Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler32

Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-

00aa004b2e24}\inprochandlerx86

Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandlerx86

 $HKCU \setminus software \setminus classes \setminus clsid \setminus \{7c857801-7381-11cf-884d-11c$ Opens key:

00aa004b2e24}\localserver

Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\localserver

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

options\wbemsvc.dll

Opens key: HKCU\software\classes\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}

HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887} Opens key: Opens key: HKCU\software\classes\interface\{d4781cd6-e5d3-44df-ad94-

930efe48a887}\proxystubclsid32

 $HKCR \verb|\| interface \verb|\| \{d4781cd6-e5d3-44df-ad94-930efe48a887\} \verb|\| proxystubclsid32|$ Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus interface \setminus \{9556dc99 - 828c - 11cf - a37e - 00aa003240c7\}$

Opens key: HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7} Opens key: HKCU\software\classes\interface\{9556dc99-828c-11cf-a37e-

00aa003240c7}\proxystubclsid32

HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32 Opens kev: Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}

Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea} HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-Opens key:

ce99a996d9ea}\treatas

 $HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\treatas$ Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-Opens kev:

ce99a996d9ea}\inprocserver32

 $HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\ \ in procserver 32$ Opens key:

HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-Opens key:

ce99a996d9ea}\inprocserverx86

Opens key: $HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\tinprocserverx86$

Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\localserver32

HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\localserver32 Opens key:

HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-Opens kev:

ce99a996d9ea}\inprochandler32

Opens key: $HKCR\clsid\d68af00a-29cb-43fa-8504-ce99a996d9ea\$ \inprochandler32

Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\inprochandlerx86

Opens key: $HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\tinprochandlerx86$

HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-Opens kev:

ce99a996d9ea}\localserver

HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\localserver Opens kev:

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

options\msvcp60.dll

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

options\wldap32.dll

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

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

options\ntdsapi.dll

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

options\fastprox.dll

Opens key: HKCU\software\classes\interface\{027947e1-d731-11ce-a357-00000000001}

Opens key: $HKCR \setminus \{027947e1-d731-11ce-a357-00000000001\}$

```
Opens key: HKCU\software\classes\interface\{027947e1-d731-11ce-a357-
```

00000000001}\proxystubclsid32

 $\label{lem:continuous} Opens \ key: \\ HKCR \ interface \ \{027947e1-d731-11ce-a357-00000000001\} \ proxystubclsid32 \\ Opens \ key: \\ HKCU \ software \ classes \ clsid \ \{1b1cad8c-2dab-11d2-b604-00104b703efd\} \\$

 Opens key:
 HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}

 Opens key:
 HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604

00104b703efd}\treatas

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\treatas Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprocserver32

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32

Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprocserverx86

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\localserver32

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\localserver32

Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprochandler32

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler32

Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprochandlerx86

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\localserver

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\localserver

Opens key: HKCU\software\classes\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}

Opens key: $\begin{tabular}{ll} HKCR\interface \{1c1c45ee-4395-11d2-b60b-00104b703efd\} \\ Opens key: \\ HKCU\software \classes \interface \{1c1c45ee-4395-11d2-b60b-00104b703efd\} \\ \end{tabular}$

00104b703efd}\proxystubclsid32

Opens key: $\label{eq:hccn} \begin{tabular}{ll} HKCR\interface \ \{1c1c45ee-4395-11d2-b60b-00104b703efd\} \ proxystubclsid32 \ Opens key: \\ HKCU\software \ classes \ interface \ \{423ec01e-2e35-11d2-b604-00104b703efd\} \ proxystubclsid32 \ prox$

Opens key: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}
Opens key: HKCU\software\classes\interface\{423ec01e-2e35-11d2-b604-

00104b703efd}\proxystubclsid32

Opens key: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat] Oueries value:

 $HKLM \verb|\software| policies \verb|\microsoft| windows \verb|\safer| code identifiers[transparentenabled]|$

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

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

nt\currentversion\compatibility32[6f2064e626e4383a5d8a9c0bdb8e9ddf]

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

compatibility[6f2064e626e4383a5d8a9c0bdb8e9ddf]

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

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

manager[criticalsectiontimeout]

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

Queries value: HKCR\interface[interfacehelperdisableall]

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

00000000046}[interfacehelperdisableall]

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

00000000046}[interfacehelperdisableallforole32]

Queries value: HKCU\control panel\desktop[multiuilanguageid]
Queries value: HKLM\software\microsoft\ctf\systemshared[cuas]
Queries value: HKCU\keyboard layout\toggle[language hotkey]
Queries value: HKCU\keyboard layout\toggle[hotkey]
Queries value: HKCU\keyboard layout\toggle[layout hotkey]
Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]
Queries value: HKLM\system\currentcontrolset\control\session

manager[safeprocesssearchmode]

Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
Queries value: HKCU\software\microsoft\ctf[disable thread input manager]
Queries value: HKLM\system\currentcontrol\set\control\nls\codepage[932]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[949]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[950]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[936]

Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3] HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4] Oueries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]

```
Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midill
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
 Queries 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\software\microsoft\windows nt\currentversion\drivers32[aux4]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
 Oueries value:
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
 Queries value:
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
 Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
                           HKLM\system\currentcontrolset\services\disk\enum[0]
 Queries value:
 Queries value:
                           HKCU\control panel\desktop[smoothscroll]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disableimprovedzonecheck]
                           HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_protocol_lockdown[6f2064e626e4383a5d8a9c0bdb8e9ddf.exe]
 Queries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
 Oueries value:
                           HKLM\system\currentcontrolset\control\wmi\securitv[df8480a1-7492-4f45-
ab78-1084642581fb1
                           Oueries value:
0000-0000000000000]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[secureprotocols]
                           HKLM\software\policies\microsoft\internet
 Queries value:
explorer\main[security_hklm_only]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablekeepalive]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[idnenabled]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[cachemode]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[enablehttp1 1]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[enablenegotiate]
 Queries value:
                           \label{lem:hkcu} \verb+KCU\+software\+microsoft\+windows\+currentversion\+internet
settings[disablebasicoverclearchannel]
 Queries value:
                           HKCU\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
                           HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[clientauthbuiltinui]
 Queries value:
                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[syncmode5]
                           \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
 Oueries value:
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache[signature]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
```

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

Oueries value:

```
settings\5.0\cache\content[peruseritem]
                          HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\content[peruseritem]
 Queries value:
                          HKLM\system\setup[systemsetupinprogress]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cacheprefix]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\cookies[peruseritem]
                          HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\cookies[peruseritem]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\cookies[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\cookies[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\history[peruseritem]
                          \label{lem:hklm} \verb+ HKLM \+ software \+ microsoft \+ windows \+ current version \+ internet
 Oueries value:
settings\5.0\cache\history[peruseritem]
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Queries value:
folders[history]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\history[cacheprefix]
                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
 Oueries value:
settings\5.0\cache\history[cachelimit]
                          HKLM\software\microsoft\rpc[maxrpcsize]
 Oueries value:
 Queries value:
HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachepath]
                          \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ internet} \end{tabular}
 Queries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cacheoptions]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cachepath]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cacherepair]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachepath]
                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\ietld[cacherepair]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
                          \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{$microsoft$} \windows \current version \internet. } \end{tabular}
 Queries value:
settings\5.0\cache\extensible cache\ietld[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\ietld[cachelimit]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
```

```
Oueries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
 Queries value:
                             \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
                             \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
 Queries value:
                             \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\privacie:[cacherepair]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries 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
 Oueries 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]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
                             HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disableworkerthreadhibernation]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablereadrange]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketsendbufferlength]
 Oueries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[keepalivetimeout]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxhttpredirects]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
                             HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsperserver]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
 Queries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsperproxy]
 Oueries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
                             HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connecttimeout]
 Oueries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
 Queries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings[connectretries]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendtimeout]
 Queries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
                             HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[receivetimeout]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablentlmpreauth]
                             \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
 Queries value:
settings[scavengecachelowerbound]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[certcachenovalidate]
 Queries value:
                             \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache[scavengecachefilelifetime]
 Queries value:
                             \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings\5.0\cache[scavengecachefilelimit]
                             HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                             \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[httpdefaultexpirytimesecs]
 Queries value:
                             \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[ftpdefaultexpirytimesecs]
                             HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[6f2064e626e4383a5d8a9c0bdb8e9ddf.exe]
                             HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
 Queries value:
                             \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
```

```
settings[disablecachingofsslpages]
 Oueries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
  Queries value:
                             \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[disablent4rascheck]
                             \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
  Oueries value:
settings[dialupuselansettings]
  Queries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value:
                             \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[sendextracrlf]
                             \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
  Oueries value:
settings[bypassftptimecheck]
                             HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[releasesocketduringauth]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
                             \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
  Queries value:
settings[releasesocketduring401auth]
                             HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[wpadsearchalldomains]
                             HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablelegacypreauthasserver]
                             {\tt HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus internet}
  Queries value:
settings[disablelegacypreauthasserver]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                             HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasshttpnocachecheck]
                             \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
  Queries value:
settings[bypasssslnocachecheck]
                             HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasssslnocachecheck]
                             HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[enablehttptrace]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
                             HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[nocheckautodialoverride]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Queries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                             HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[sharecredswithwinhttp]
                             \label{lem:hkcu} \verb+kkcu+ software \verb+microsoft+ windows \verb+current version+ internet+ \\
  Queries value:
settings[mimeexclusionlistforcache]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
                             HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[dnscacheenabled]
  Queries value:
                             \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[dnscacheentries]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
                             HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonpost]
                             HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnalwaysonpost]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
                             HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonbadcertsending]
  Oueries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
  Oueries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
                             HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonhttpstohttpredirect]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Oueries value:
```

Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000002[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem] Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries \ 0000000000008 \ [packed catalog item] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
 Oueries value:
- $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws 2_32 spin count]$
- Queries value: HKCU\software\microsoft\windows\currentversion\internet
- settings[globaluseroffline]
- Queries value: HKCU\software\microsoft\windows\currentversion\internet
- settings[enableautodial]
- Queries value: HKLM\software\microsoft\windows\currentversion\internet
- settings[urlencoding]
- Queries value: HKCU\software\microsoft\windows\currentversion\internet

```
settings[truncatefilename]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[badproxyexpirestime]
 Queries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32maxnumrequestretries]
 Queries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32requestretrytimeout]
                         HKLM\software\microsoft\tracing[enableconsoletracing]
 Oueries value:
 Oueries value:
                          HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
 Oueries value:
                          HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
 Oueries value:
                          HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
 Queries value:
                          HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
 Queries value:
                          HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
 Oueries value:
                          HKLM\software\microsoft\tracing\rasapi32[filedirectory]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common appdata]
                          HKI M\software\microsoft\windows
 Oueries value:
nt\currentversion\winlogon[userenvdebuglevel]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\winlogon[chkaccdebuglevel]
 Queries value:
                          HKLM\system\currentcontrolset\control\productoptions[producttype]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[personal]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local settings]
                          HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\winlogon[rsopdebuglevel]
                          HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
 Queries value:
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\profilelist[profilesdirectory]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\profilelist[allusersprofile]
                          HKLM\software\microsoft\windows
nt\currentversion\profilelist[defaultuserprofile]
                         HKLM\software\microsoft\windows\currentversion[programfilesdir]
 Oueries value:
                          HKLM\software\microsoft\windows\currentversion[commonfilesdir]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
 Oueries value:
1757981266-507921405-1957994488-1003[profileimagepath]
                          HKCU\software\microsoft\windows
nt\currentversion\winlogon[parseautoexec]
 Queries value:
                          \label{thm:local_explorer} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \user shell \end{tabular}
folders[appdata]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[migrateproxy]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[proxyenable]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[proxyoverride]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[autoconfigurl]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\connections[defaultconnectionsettings]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[6f2064e626e4383a5d8a9c0bdb8e9ddf.exe]
 Oueries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[*]
 Queries value:
                         HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
 Oueries value:
                         HKLM\software\microsoft\rpc\securityservice[10]
 Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
                          \label{local-objective} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\ietld[ietlddllversionlow]}} \label{local-objective}
 Queries value:
                          HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
                          HKLM\software\policies\microsoft\internet
 Queries value:
explorer\security[disablesecuritysettingscheck]
 Queries value:
                          HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
 Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]
HKLM\svstem\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]
 Queries value:
                          HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]
 Queries value:
HKLM\system\currentcontrol\set\control\lsa\sspicache\msapsspc.dll[version]
 Queries value:
                          HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]
 Oueries value:
```

Queries value: Queries value:

Oueries value:

HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]

HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]

Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[flags] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid] HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type] Oueries value: Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize] HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name] Oueries value: Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[flags] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities] HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid] Oueries value: Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type] Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize] $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Queries value: settings\zones\2[flags] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\3[flags] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\4[flags] HKCU\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_localmachine_lockdown[6f2064e626e4383a5d8a9c0bdb8e9ddf.exe] HKCU\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_localmachine_lockdown[*] HKLM\software\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_localmachine_lockdown[6f2064e626e4383a5d8a9c0bdb8e9ddf.exe] HKLM\software\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_localmachine_lockdown[*] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[createuricachesize] Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[createuricachesize] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[enablepunycode] $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus internet$ Queries value: settings[enablepunycode] $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Queries value: settings\zonemap[autodetect] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\3[1a10] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [prioritize record data]$ Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Queries value: Queries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[screenbadtlds] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Queries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Queries value:

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

 $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [register adapter name]$

Queries value:

Queries value:

```
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
   Queries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
                                              HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
   Queries value:
                                              HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
   Oueries value:
                                              HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [maxcachettl]
   Queries value:
   Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [maxnegative cachettl]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
   Oueries value:
Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [max cached sockets]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
                                              HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
   Oueries value:
   Oueries value:
c7d49d7cecdc}[enabledhcp]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[leaseobtainedtime]
   Oueries value:
c7d49d7cecdc}[leaseterminatestime]
   Queries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4404b, and a system \ begin{center} 16325b0b-4636-4303-abe3-4404b, and a system \ begin{center} 16325b0b-4636-4404b, and a system \ begin{center} 16325b0b-4636-4404b, and a system \ begin{center} 
c7d49d7cecdc}[dhcpserver]
                                              HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
   Oueries value:
   Queries value:
                                              HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[queryadaptername]
   Queries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-a
c7d49d7cecdc}[disableadapterdomainname]
c7d49d7cecdc}[registrationenabled]
   Queries value:
c7d49d7cecdc}[registeradaptername]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registrationmaxaddresscount]
   Queries value:
c7d49d7cecdc}[maxnumberofaddressestoregister]
```

Oueries value: c7d49d7cecdc}[domain] c7d49d7cecdc}[dhcpdomain] Oueries value: c7d49d7cecdc}[ipautoconfigurationenabled] c7d49d7cecdc}[addresstype] Queries value: $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-4404, and an armonic set \ services \ tcpip \ parameters \ interfaces \ tcpip \ parameters \ terrange \ tcpip \ parameters \ tcpip \ parameters$ c7d49d7cecdc}[nameserver] Oueries value: $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4300-abe3-4300-a$ c7d49d7cecdc}[dhcpnameserver] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder] HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong Queries value: cryptographic provider[type] HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong Queries value: cryptographic provider[image path] HKLM\software\microsoft\cryptography[machineguid] Queries value: Queries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel] Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance] HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname] HKCU\software\microsoft\internet Queries value: explorer\ietld\lowmic[ietlddllversionlow] HKCU\software\microsoft\internet Queries value: explorer\ietld\lowmic[ietlddllversionhigh] HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[{aeba21fa-782a-4a90-978d-b72164c80120}] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[privacyadvanced] HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps] Queries value: Oueries value: HKLM\software\microsoft\windows\currentversion\explorer[maximizeapps] Queries value: $\label{thm:local} \verb|HKCU| software \verb|\microsoft| windows \verb|\currentversion| policies \verb|\explorer| [nonethood]| \\$ Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{11016101-e366-4d22bc06-4ada335c892b}[suppressionpolicy] Oueries value: ba4f-00a0c91eedba}[suppressionpolicy] Oueries value: $HKLM \ software \ microsoft \ windows \ current version \ explorer \ desktop \ names pace \ \{450d8fba-ad25-11d0-da8fba-ad25-11d0-da8fba-ad25-11d0-da8fba-ad25-da$ 98a8-0800361b1103}[suppressionpolicv] Oueries value: 9f08-00aa002f954e}[suppressionpolicy] Oueries value: 83f2-00a0c90dc849}[suppressionpolicy] $HKCR\clsid\{20d04fe0-3aea-1069-a2d8-$ Queries value: 08002b30309d}\shellfolder[wantsparsedisplayname] HKCR\clsid\{208d2c60-3aea-1069-a2d7-Oueries value: 08002b30309d}\shellfolder[wantsparsedisplayname] Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[wantsparsedisplayname] HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[] Queries value: Oueries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[loadwithoutcom]

HKLM\software\microsoft\windows\currentversion\shell

HKCU\software\microsoft\windows\currentversion\shell

extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]

extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]

Oueries value:

Oueries value:

Oueries value:

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

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

extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}

Queries value: $\label{local-objective} \verb|HKCU| software \verb|microsoft| windows \verb|currentversion| shell \\$

extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}

0x4011

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

manager\appcompatibility[disableappcompat]

Oueries value: HKLM\software\microsoft\com3[com+enabled]

Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess] Oueries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]

HKLM\software\microsoft\com3[regdbversion] Oueries value: Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\inprocserver32[inprocserver32]

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

Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\inprocserver32[threadingmodel]

HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe[] Queries value: Queries value: HKLM\software\microsoft\internet explorer\setup[iexplorelastmodifiedlow]

Queries value: HKLM\software\microsoft\internet

explorer\setup[iexplorelastmodifiedhigh]

HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib[] Queries value: Queries value: HKLM\software\microsoft\internet explorer\setup[installstarted]

 $HKCR \verb|\interface| \{b722bccb-4e68-101b-a2bc-00aa00404770\} \verb|\proxystubclsid32[]| \\$ Oueries value: Queries value: HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32[] Queries value: HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32[] $HKCR \verb|\interface| \{93f2f68c-1d1b-11d3-a30e-00c04f79abd1\} \verb|\proxystubclsid32[]| \\$ Oueries value:

HKCR\clsid\{11016101-e366-4d22-bc06-Queries value:

4ada335c892b}\shellfolder[wantsparsedisplayname]

HKCR\clsid\{1f4de370-d627-11d1-ba4f-Queries value:

00a0c91eedba}\shellfolder[wantsparsedisplayname]

Queries value: HKCR\clsid\{450d8fba-ad25-11d0-98a8-

0800361b1103}\shellfolder[wantsparsedisplayname]

HKCR\clsid\{645ff040-5081-101b-9f08-

00aa002f954e}\shellfolder[wantsparsedisplayname]

HKCR\clsid\{e17d4fc0-5564-11d1-83f2-Oueries value:

00a0c90dc849}\shellfolder[wantsparsedisplayname]

HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32[] Queries value:

Oueries value: HKCR\clsid\{aeb6717e-7e19-11d0-97ee-

00c04fd91972}\inprocserver32[loadwithoutcom]

Queries value: HKCR\.exe[] HKCR\.asp[] Oueries value: HKCR\.bat[] Oueries value: Queries value: HKCR\.cer[] HKCR\.chm[] Oueries value: Queries value: HKCR\.cmd[] HKCR\.com[] Oueries value: HKCR\.cpl[] Queries value: HKCR\.crt[] Oueries value:

HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-Oueries value:

00c04fb6bfc4}\inprocserver32[inprocserver32]

 $HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\nprocserver32[]$ Queries value:

Oueries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[appid]

Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\inprocserver32[threadingmodel]

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

settings[specialfolderscachesize]

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

settings[specialfolderscachesize]

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

settings\zones\0[1806]

Oueries value:

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

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

HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[] Oueries value:

Queries value: HKLM\system\wpa\pnp[seed] HKLM\system\setup[osloaderpath] Oueries value: Queries value: HKLM\system\setup[systempartition]

HKLM\software\microsoft\windows\currentversion\setup[sourcepath] Oueries value:

Oueries value:

HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]

Queries value:

HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]

HKLM\software\microsoft\windows\currentversion\setup[drivercachepath] Queries value:

HKLM\software\microsoft\windows\currentversion[devicepath] Oueries value: Oueries value: HKLM\software\microsoft\windows\currentversion\setup[loglevell Oueries value: HKLM\software\microsoft\windows\currentversion\setup[logpath]

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{f90255c2-6bc4-f9025c2-6bc4-f90255c2-6bc4-f90255c2-6bc4-f9025c2-6bc4-f9025c2-6bc4-f90255c2-6bc4-f9025c2-6bc4-f$

11e3-9fc7-806d6172696f}[data]

Oueries value: $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mountpoints 2 \setminus cpc \setminus volume \setminus \{f90255c2-6bc4-facet \} \cap facet = facet \}$ 11e3-9fc7-806d6172696f}[generation] Queries value: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}[drivemask] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[forceactivedesktopon] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu] HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden] Oueries value: Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext] Queries value: $HKCU \ software \ microsoft \ windows \ current version \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ advanced \ advanced \ advanced \ (explorer \ advanced \ advanced \ advanced \ advanced \ (explorer \ advanced \ advanced \ advanced \ advanced \ (explorer \ advanced \ advanced \ advanced \ advanced \ (explorer \ advanced \ advanced \ advanced \ advanced \ (explorer \ advanced \ advanced \ advanced \ advanced \ (explorer \ advanced \ advanced \ advanced \ advanced \ (explorer \ advanced \ advanced \ advanced \ advanced \ advanced \ (explorer \ advanced \ advanced \ advanced \ advanced \ advanced \ advanced \ (explorer \ advanced \ advanced \ advanced \ advanced \ advanced \ (explorer \ advanced \ (explorer \ advanced \ (explorer \ advanced \ advanced \ advanced \ advanced \ advanc$ HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons] Queries value: $HKCU \ software \ `microsoft \ `windows \ `current version \ `explorer \ `advanced \ [mapnet drvbtn]" \ in the context of th$ HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess] Oueries value: HKCR\directory[docobject] Oueries value: HKCR\directory[browseinplace] Queries value: Queries value: HKCR\directory[isshortcut] Queries value: HKCR\directory[alwaysshowext] HKCR\directory[nevershowext] Oueries value: Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions] HKCR\exefile[docobject] Oueries value: Queries value: HKCR\exefile[browseinplace] Queries value: HKCR\exefile[isshortcut] Oueries value: HKCR\exefile[alwaysshowext] Queries value: HKCR\exefile[nevershowext] Queries value: HKCR\exefile\shell[] Oueries value: HKCR\exefile\shell\open\command[] Oueries value: HKCR\exefile\shell\open\command[command] HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-Queries value: 1757981266-507921405-1957994488-1003[flags] Queries value: $HKLM \ \ \, nt\ \ \, \$ 1757981266-507921405-1957994488-1003[state] Oueries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003[userpreference] $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} is on \begin{tabular}{ll} HKLM \end{ta$ Oueries value: 1757981266-507921405-1957994488-1003[centralprofile] Queries value: $HKLM \ \ \, nt\ \ \, \$ 1757981266-507921405-1957994488-1003[profileloadtimelow] HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-Oueries value: 1757981266-507921405-1957994488-1003[profileloadtimehigh] Oueries value: HKCU\software\microsoft\windows\shellnoroam\muicache[langid] Oueries value: HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\cmd.exe] Queries value: Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[disallowrun]

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer[norunasinstall prompt]$

HKLM\system\wpa\mediacenter[installed]

Queries value:

Queries value:

Oueries value:

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

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

Queries value:

 $HKLM\software \policies \microsoft\windows \safer\code identifiers \noindent \paths \da3f824-d8cb-441b-834d-be2efd2c1a33\paths \paths \paths$

Queries value:

 $HKLM\software \policies \microsoft\windows \safer\code identifiers \noindent \paths \quad the 2efd2c1a33\paths \paths \$

Queries value:

Oueries value:

Queries value:

Queries value:

Queries value:

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

Queries value:

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \policies \microsoft \windows \safer \code identifiers \oldshes \{94e3e076-8f53-42a5-8411-085bcc18a68d} \ [hashalg]$

Queries value:

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

Queries value:

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ \ \ dc971ee5-44eb-4fe4-ae2e-b91490411bfc \ [itemdata]$

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}\ [hashalg]$

Oueries value:

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

Queries value:

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

Queries value:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [default level]$

Queries value:

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

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

folders[cache]

Oueries value:

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

Queries value: HKCU\software\microsoft\visual basic\6.0[allowunsafeobjectpassing]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[cmd]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[cmd]

Queries value: HKCU\software\microsoft\multimedia\audio[systemformats]

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\drivers32[msacm.imaadpcm]

Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[fdwsupport] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags] Oueries value: $HKLM \verb|\software\microsoft\audiocompression| manager \verb|\driver| cache \verb|\msacm.imaadpcm[aformattagcache]| aformattagcache]| the software \verb|\msacm.imaadpcm[aformattagcache]| and the software$ Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cfiltertags] HKLM\software\microsoft\windows Oueries value: nt\currentversion\drivers32[msacm.msadpcm] Oueries value: Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cformattags] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[aformattagcache] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cfiltertags] HKLM\software\microsoft\windows Queries value: nt\currentversion\drivers32[msacm.msg711] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[fdwsupport] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cformattags] Queries value: Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cfiltertags] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msgsm610] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[fdwsupport] HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cformattags] Oueries value: Oueries value: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. msgsm610[cfilter tags]$ HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.trspch] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[aformattagcache] Oueries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msg723] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[fdwsupport] Queries value: Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[aformattagcache] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cfiltertags] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msaudio1] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cformattags] Oueries value: $HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} which is a constant a graph \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lklm} \label{lkm} \label{lkm}$ Queries value: $HKLM \verb|\software\microsoft\audiocompression manager\driver cache \verb|\msaudio1[cfiltertags]| \\$ Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.sl_anet] Queries value: $HKLM \label{lem:hklm} Which is a constant, which$

Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cformattags] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[aformattagcache] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cfiltertags] HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2] Oueries value: Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport]

Oueries value:

 $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ macm. iac2 [cformattags]$

```
Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[aformattagcache]
   Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cfiltertags]
                                               HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.l3acm]
   Oueries value:
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[fdwsupport]
   Oueries value:
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ macm. 13 acm [cformattags]
   Oueries value:
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. 13 acm [a formattag cache]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags]
   Oueries value:
                                               HKCU\software\microsoft\multimedia\audio compression
manager\msacm[nopcmconverter]
   Queries value:
                                               HKCU\software\microsoft\multimedia\audio compression manager\priority
v4.00[prioritv1]
   Queries value:
                                               HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
   Queries value:
                                               HKCU\control panel\desktop[lamebuttontext]
                                               HKLM\software\microsoft\command processor[disableunccheck]
   Oueries value:
   Queries value:
                                               HKLM\software\microsoft\command processor[enableextensions]
   Queries value:
                                               HKLM\software\microsoft\command processor[delayedexpansion]
                                               HKLM\software\microsoft\command processor[defaultcolor]
   Oueries value:
   Queries value:
                                               HKLM\software\microsoft\command processor[completionchar]
   Queries value:
                                               HKLM\software\microsoft\command processor[pathcompletionchar]
   Oueries value:
                                               HKLM\software\microsoft\command processor[autorun]
   Queries value:
                                               HKCU\software\microsoft\command processor[disableunccheck]
   Queries value:
                                               HKCU\software\microsoft\command processor[enableextensions]
   Oueries value:
                                               HKCU\software\microsoft\command processor[delayedexpansion]
   Queries value:
                                               HKCU\software\microsoft\command processor[defaultcolor]
   Queries value:
                                               HKCU\software\microsoft\command processor[completionchar]
   Queries value:
                                               HKCU\software\microsoft\command processor[pathcompletionchar]
   Queries value:
                                               HKCU\software\microsoft\command processor[autorun]
   Queries value:
                                               HKLM\system\currentcontrolset\control\nls\locale[00000409]
                                               HKLM\system\currentcontrolset\control\nls\language groups[1]
   Oueries value:
   Queries value:
                                               HKLM\software\microsoft\windows
nt\currentversion\compatibility32[tasklist]
                                               HKLM\software\microsoft\windows nt\currentversion\ime
   Queries value:
compatibility[tasklist]
                                               HKLM\software\microsoft\wbem\cimom[logging]
   Queries value:
                                               HKLM\software\microsoft\wbem\cimom[logging directory]
   Oueries value:
   Queries value:
                                               HKLM\software\microsoft\wbem\cimom[log file max size]
   Queries value:
                                               HKLM\software\microsoft\ole[maximumallowedallocationsize]
                                               {\tt HKLM \ } system \verb|\ current control \ \\ lsa[every one includes an ony mous]
   Oueries value:
                                               HKCR\clsid\{4590f811-1d3a-11d0-891f-
   Oueries value:
00aa004b2e24}\inprocserver32[inprocserver32]
                                               HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\nprocserver32[]
   Oueries value:
   Queries value:
                                               HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[appid]
                                               HKCR\clsid\{4590f811-1d3a-11d0-891f-
   Oueries value:
00aa004b2e24}\inprocserver32[threadingmodel]
                                               HKLM\software\microsoft\wbem\cimom[repository directory]
   Oueries value:
                                               HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[appid]
   Oueries value:
                                               \label{local-equation} \mbox{HKCR} $$ \arrowvert a HKCR \arrowve
   Queries value:
                                               HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[localservice]
   Queries value:
   Oueries value:
                                               \label{local-eq:hkcr} \begin{tabular}{ll} HKCR \end{tabular} $$\operatorname{HKCR} \arrowvert = (f309ad18-d86a-11d0-a075-00c04fb68820) \end{tabular} $$\operatorname{HKC
   Queries value:
                                               HKCR\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[inprocserver32]
                                               HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[]
   Oueries value:
                                               HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[appid]
   Oueries value:
                                               HKCR\clsid\{7c857801-7381-11cf-884d-
   Queries value:
00aa004b2e24}\inprocserver32[threadingmodel]
                                               HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32[]
   Oueries value:
   Queries value:
                                               HKCR \ interface \ \{9556dc99-828c-11cf-a37e-00aa003240c7\} \ proxystubclsid32[]
   Queries value:
                                               HKCR\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[inprocserver32]
                                               HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32[]
   Oueries value:
                                               HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[appid]
   Queries value:
                                               HKCR\clsid\{d68af00a-29cb-43fa-8504-
   Oueries value:
ce99a996d9ea}\inprocserver32[threadingmodel]
                                               HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
   Oueries value:
   Queries value:
                                               HKLM\software\microsoft\wbem\cimom[processid]
                                               HKLM\software\microsoft\wbem\cimom[enableprivateobjectheap]
   Oueries value:
   Oueries value:
                                               HKLM\software\microsoft\wbem\cimom[contextlimit]
   Oueries value:
                                               HKLM\software\microsoft\wbem\cimom[objectlimit]
   Queries value:
                                               HKLM\software\microsoft\wbem\cimom[identifierlimit]
                                               HKCR\interface\{027947e1-d731-11ce-a357-00000000001}\proxystubclsid32[]
   Oueries value:
   Queries value:
                                               HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[inprocserver32]
   Oueries value:
                                               HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32[]
                                               HKCR\clsid{1b1cad8c-2dab-11d2-b604-00104b703efd}[appid]
   Oueries value:
   Queries value:
                                               HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[threadingmodel]
```

 $HKCR \ interface \ \{1c1c45ee-4395-11d2-b60b-00104b703efd\} \ \ proxystubclsid32[]$

Queries value:

Queries value: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32[]

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

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

folders[cache]

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

folders[cookies]

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

folders[history]

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

folders[common appdata]

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

folders[appdata]

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

settings[proxyenable]

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

settings\connections[savedlegacysettings]

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

settings\zonemap[proxybypass]

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

settings\zonemap[intranetname]

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

settings\zonemap[uncasintranet]

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

settings\zonemap[autodetect]

Value changes:

806d6172696f}[baseclass]