# Malware Analysis Appliance by Blue Coat Systems, Inc.

#### Task Details

Host: mag2, Sample ID: 3318, Task ID: 780

Task ID: 780 Risk Level: 10

Date Processed: 2016-05-18 10:37:23 (UTC)

Processing Time: 61.36 seconds Virtual Environment: IntelliVM

**Execution Arguments:** "c:\windows\temp\f0da8593d29e9b367fda7028db12cab0.exe"

Sample ID: Type: basic Owner: admin

f0da8593d29e9b367fda7028db12cab0 Label:

Date Added: 2016-05-18 10:30:50 (UTC)

PE32:win32:gui File Type: File Size: 323584 bytes

f0da8593d29e9b367fda7028db12cab0 MD5:

08257c7a15283c59cc8cd4e76c326b009fac61607d7c9d1def559b41b079f8ce SHA256:

Description: None

#### Pattern Matching Results

5 PE: Contains compressed section

3 Program causes a crash [Info] 10 Creates malicious mutex: QQLogger [Backdoor, keylogger]

4 Reads process memory

#### Process/Thread Events

C:\WINDOWS\Temp\f0da8593d29e9b367fda7028db12cab0.exe Creates process:

["c:\windows\temp\f0da8593d29e9b367fda7028db12cab0.exe"]

C:\WINDOWS\system32\dwwin.exe [C:\WINDOWS\system32\dwwin.exe -x -s 196] Creates process:

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

Reads from process: PID:344 C:\WINDOWS\Temp\f0da8593d29e9b367fda7028db12cab0.exe

#### Named Object Events

Creates mutex: \BaseNamedObjects\setup\_fat32sys Creates mutex: \BaseNamedObjects\SHIMLIB\_LOG\_MUTEX

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

1957994488-1003

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

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

1957994488-1003

Creates mutex:

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

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

Creates mutex:

1957994488-1003 Creates mutex: \BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-

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

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

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 event: \BaseNamedObjects\userenv: User Profile setup event

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

Creates semaphore: \BaseNamedObjects\MsoDWExclusive344

### File System Events

Creates C:\Documents and Settings\Admin\Local Settings\Temp\cc9\_appcompat.txt Creates: C:\Documents and Settings\Admin\Local Settings\Temp\A5DEBD.dmp

Opens: C:\WINDOWS\Prefetch\F0DA8593D29E9B367FDA7028DB12C-0B408EFB.pf

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

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

Controls\_6595b64144ccf1df\_6.0.2600.5512\_x-ww\_35d4ce83

Opens: C:\WINDOWS\WinSxS\x86\_Microsoft.Windows.Common-

Controls\_6595b64144ccf1df\_6.0.2600.5512\_x-ww\_35d4ce83\comctl32.dll

Opens: C:\WINDOWS\WindowsShell.Manifest C:\WINDOWS\WindowsShell.Config Opens: Opens: C:\WINDOWS\system32\comctl32.dll

Opens: C:\WINDOWS\system32\comctl32.dll.124.Manifest Opens: C:\WINDOWS\system32\comctl32.dll.124.Config

```
C:\WINDOWS\Temp\f0da8593d29e9b367fda7028db12cab0.exe
Opens:
Opens:
                       C:\WINDOWS\system32\faultrep.dll
Opens:
                       C:\WINDOWS\system32\winsta.dll
Opens:
                       C:\WINDOWS\system32\netapi32.dll
Opens:
                       C:\WINDOWS\system32\wtsapi32.dll
Opens:
                       C:\WINDOWS\system32\setupapi.dll
Opens:
Opens:
                       C:\WINDOWS
                       C:\WINDOWS\system32\apphelp.dll
Opens:
Opens:
                       C:\WINDOWS\Temp\c074f5c6-e4da-43be-9c8f-5a3732327244
Opens:
                       C:\Documents and Settings\Admin\Local Settings\Temp
Opens:
                       C:\WINDOWS\Temp
Opens:
                       C:\Documents and Settings\Admin\Local Settings\Temp\cc9_appcompat.txt
Opens:
                       C:\WINDOWS\system32
Opens:
                       C:\WINDOWS\system32\kernel32.dll
                       C:\WINDOWS\system32\dwwin.exe
Opens:
Opens:
                       C:\WINDOWS\AppPatch\sysmain.sdb
                       C:\WINDOWS\AppPatch\systest.sdb
Opens:
Opens:
                       C:\WINDOWS\system32\dwwin.exe.Manifest
Opens:
                       C:\WINDOWS\Prefetch\DWWIN.EXE-30875ADC.pf
Opens:
                       C:\WINDOWS\AppPatch
Opens:
                       C:\WINDOWS\system32\1033
Opens:
Opens:
                       C:\WINDOWS\system32\en-US
Opens:
                       C:\WINDOWS\WinSxS
Opens:
                       C:\WINDOWS\system32\ntdll.dll
Opens:
                       C:\WINDOWS\system32\unicode.nls
Opens:
                       C:\WINDOWS\system32\locale.nls
Opens:
                       C:\WINDOWS\system32\sorttbls.nls
Opens:
                       C:\WINDOWS\system32\advapi32.dll
Opens:
                       C:\WINDOWS\system32\rpcrt4.dll
Opens:
                       C:\WINDOWS\system32\secur32.dll
Opens:
                       C:\WINDOWS\system32\gdi32.dll
Opens:
                       C:\WINDOWS\system32\user32.dll
Opens:
                       C:\WINDOWS\system32\oleaut32.dll
Opens:
                       C:\WINDOWS\system32\msvcrt.dll
Opens:
                       C:\WINDOWS\system32\ole32.dll
Opens:
                       C:\WINDOWS\system32\shlwapi.dll
Opens:
                       C:\WINDOWS\system32\urlmon.dll
Opens:
                       C:\WINDOWS\system32\iertutil.dll
Opens:
                       C:\WINDOWS\system32\version.dll
Opens:
                       C:\WINDOWS\system32\wininet.dll
Opens:
                       C:\WINDOWS\system32\normaliz.dll
Opens:
                       C:\WINDOWS\system32\shimeng.dll
Opens:
                       C:\WINDOWS\AppPatch\AcGenral.dll
Opens:
                       C:\WINDOWS\system32\winmm.dll
                       C:\WINDOWS\system32\msacm32.dll
Opens:
Opens:
                       C:\WINDOWS\system32\userenv.dll
Opens:
                       C:\WINDOWS\system32\uxtheme.dll
Opens:
                       C:\WINDOWS\system32\ctype.nls
Opens:
                       C:\WINDOWS\system32\sortkey.nls
Opens:
                       C:\WINDOWS\system32\win32k.sys
                       C:\WINDOWS\system32\riched20.dll
Opens:
Opens:
                       C:\WINDOWS\system32\shfolder.dll
Opens:
                       C:\WINDOWS\system32\MSCTF.dll
Opens:
                       C:\WINDOWS\system32\1033\dwintl.dll
Opens:
                       C:\WINDOWS\system32\en-US\wininet.dll.mui
Opens:
                       C:\WINDOWS\system32\ws2 32.dll
Opens:
                       C:\WINDOWS\system32\ws2help.dll
Opens:
                       C:\WINDOWS\system32\rasapi32.dll
Opens:
                       C:\WINDOWS\system32\rasman.dll
Opens:
                       C:\WINDOWS\system32\tapi32.dll
Opens:
                       C:\WINDOWS\system32\rtutils.dll
Opens:
                       C:\WINDOWS\system32\sensapi.dll
Opens:
                       C:\WINDOWS\system32\msv1_0.dll
Opens:
                       C:\WINDOWS\system32\iphlpapi.dll
Opens:
                       C:\WINDOWS\win.ini
                       C:\WINDOWS\system32\oleacc.dll
Opens:
Opens:
                       C:\WINDOWS\system32\msvcp60.dll
Opens:
                       C:\WINDOWS\system32\oleaccrc.dll
Opens:
                       C:\WINDOWS\system32\narrhook.dll
Opens:
                       C:\WINDOWS\system32\COMCTL32.DLL.124.Manifest
Opens:
                       C:\WINDOWS\system32\COMCTL32.DLL.124.Config
Opens:
                       C:\WINDOWS\system32\SHELL32.DLL.124.Manifest
Opens:
                       C:\WINDOWS\system32\SHELL32.DLL.124.Config
                       C:\WINDOWS\system32\URLMON.DLL.123.Manifest
Opens:
Opens:
                       C:\WINDOWS\system32\URLMON.DLL.123.Config
Opens:
                       C:\WINDOWS\system32\WININET.DLL.123.Manifest
Opens:
                       C:\WINDOWS\system32\WININET.DLL.123.Config
Opens:
                       C:\WINDOWS\system32\psapi.dll
Opens:
                       C:\Documents and Settings\Admin\Local Settings\Temp\A5DEBD.dmp
Opens:
                       C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
```

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

Opens:

Files\Content.IE5

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

C:\Documents and Settings\Admin\Local Settings\History\History.IE5 Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Opens:

Files\Content.IE5\index.dat

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

C:\Documents and Settings\Admin\Cookies\index.dat Opens:

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

Settings\History\History.IE5\index.dat

C:\WINDOWS\system32\TAPI32.dll.124.Manifest C:\WINDOWS\system32\TAPI32.dll.124.Config Opens:

Opens: C:\AUTOEXEC.BAT

Opens: C:\Documents and Settings\All Users\Application

Data\Microsoft\Network\Connections\Pbk

Opens: C:\WINDOWS\system32\ras

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

Data\Microsoft\Network\Connections\Pbk\

Opens: C:\WINDOWS\Fonts\sserife.fon

Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\cc9\_appcompat.txt Writes to:

C:\Documents and Settings\Admin\Local Settings\Temp\A5DEBD.dmp Reads from:

C:\WINDOWS\Temp\f0da8593d29e9b367fda7028db12cab0.exe Reads from: C:\WINDOWS\Prefetch\DWWIN.EXE-30875ADC.pf

Reads from: C:\AUTOEXEC.BAT Reads from: C:\WINDOWS\win.ini

## Windows Registry Events

HKLM\software\microsoft\pchealth\errorreporting Creates key:

Creates key: HKLM\software\microsoft\pchealth\errorreporting\exclusionlist Creates key: Creates key: HKCU\software\microsoft\windows\currentversion\internet settings

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

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

v4.00

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

folders

Creates kev: HKCU\software\microsoft\windows\currentversion\explorer\shell folders

Creates key: HKLM\software\microsoft\tracing

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

folders

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

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

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

settings\connections

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

manager[pendingfilerenameoperations]

Deletes value: HKLM\software\microsoft\pchealth\errorreporting\dw[dwfiletreeroot]

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

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

options\f0da8593d29e9b367fda7028db12cab0.exe

Opens key: HKLM\system\currentcontrolset\control\terminal server

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

options\gdi32.dll

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

options\user32.dll

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

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers

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

options\imm32.dll

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

options\ntdll.dll Opens key:

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

Opens key:

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

Opens key:

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

options\rpcrt4.dll

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

options\advapi32.dll

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

options\msvcrt.dll

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

options\shlwapi.dll

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

```
options\shell32.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
                          HKLM\software\microsoft\windows nt\currentversion\winlogon
 Opens key:
 Opens key:
                          HKI M\
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\diagnostics
                          HKLM\software\microsoft\windows\currentversion\explorer\performance
 Opens key:
 Opens key:
                          HKLM\system\setup
 Opens key:
                          HKCU\
                          HKCU\software\policies\microsoft\control panel\desktop
 Opens key:
 Opens key:
                          HKCU\control panel\desktop
 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:
                          HKCU\software\microsoft\windows\currentversion\explorer\advanced
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\languagepack
 Opens key:
                          HKLM\software\microsoft\windows\currentversion\explorer\shell folders
                          HKLM\software\microsoft\windows nt\currentversion\aedebug
 Opens kev:
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\userenv.dll
 Opens key:
                          HKLM\system\currentcontrolset\control\productoptions
                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}
 Opens key:
folders
 Opens key:
                          HKLM\software\policies\microsoft\windows\system
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\netapi32.dll
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winsta.dll
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wtsapi32.dll
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
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
                          HKLM\software\microsoft\windows\currentversion\setup\apploglevels
 Opens key:
 Opens key:
                          {\tt HKLM \ } system \verb|\ current control \ \\ computer name \verb|\ active computer name \ \\ 
 Opens key:
                          HKLM\system\currentcontrolset\services\tcpip\parameters
 Opens key:
                          HKLM\software\policies\microsoft\system\dnsclient
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
```

options\faultrep.dll

HKLM\software\policies\microsoft\pchealth\errorreporting Opens key: Opens key: HKLM\software\microsoft\pchealth\errorreporting\dw

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

Opens key: HKLM\software\microsoft\rpc

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

options\f0da8593d29e9b367fda7028db12cab0.exe\rpcthreadpoolthrottle Opens key: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKLM\system\currentcontrolset\control\computername

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

options\apphelp.dll

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

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers  $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \end{tabular} Software \end{tabular} in the current version \end{tabular} approximately approxima$ Opens key:

Opens key: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags\custom\dwwin.exe

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

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

be2efd2c1a33}

Opens key:  $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes$ 

Opens kev:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{349d35ab-37b5-462f-9b89-4666f-9b89-46666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b$ 

Opens kev:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57bb813f72dbb91}

Opens kev:

```
7c29ddecae3f}
  Opens kev:
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{94e3e076-8f53-42a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-6442a5-8411-644445-8411-644445-8411-644445-8411-64446-8411-64446-8411-64446-8411-64446-8411-64446-8411-64446-84446-84446-84446-84446-84446-84446-84464-8446-8446-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-84466-8446668-844666-84466-844666-84466-844666-844666-84466-84466-844666-84466-84466-84466-844666-8446686
085bcc18a68d}
  Opens kev:
b91490411bfc}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus urlzones
   Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus paths
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
  Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus urlzones
   Opens key:
                                           HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
   Opens key:
                                           HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
   Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus hashes
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
   Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus has hes
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
   Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus urlzones
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
   Opens key:
                                           HKCU\software\microsoft\windows\currentversion\explorer\shell folders
   Opens key:
                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dwwin.exe
  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\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\iertutil.dll
                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens kev:
options\urlmon.dll
```

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

Opens key:

Opens key: options\shimeng.dll Opens key:

options\normaliz.dll
 Opens key:

options\wininet.dll

options\winmm.dll
 Opens key:

```
options\msacm32.dll
```

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

options\uxtheme.dll

Opens key: HKLM\software\microsoft\ole

Opens key: HKCR\interface

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

HKLM\software\microsoft\oleaut Opens key:

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

Opens key: HKCU\software\classes\

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

Opens key: HKCR\protocols\name-space handler

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

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

settings

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

settings

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_protocol\_lockdown HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_protocol\_lockdown

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

settings\

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

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_ignore\_policies\_zonemap\_if\_esc\_enabled\_kb918915

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature\_ignore\_policies\_zonemap\_if\_esc\_enabled\_kb918915 HKLM\software\policies\microsoft\windows\currentversion\internet Opens key:

settings\zonemap\domains\

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

settings\zonemap\domains\

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

settings\zonemap\ranges\

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

settings\zonemap\ranges\

HKCU\software\microsoft\internet Opens key: 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: HKLM\software\microsoft\windows nt\currentversion\drivers32

Opens key:

Opens key:  $HKLM \verb|\software\microsoft\audiocompression manager \verb|\drivercache| \\$ 

Opens kev:

 $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.ima adpcmark to the first of the compression of the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus driver$ 

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

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

Opens key:

 $HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus msacm. \, msgsm610$ 

 $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ audiocompression manager\+ driver cache\+ msacm.trspch$ Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723 Opens key:

Opens key:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl\_anet

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

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

Opens key: HKCU\software\microsoft\office\10.0\common\debug

Opens key: HKLM\software\microsoft\oasys\oaclient

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

options\riched20.dll

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

options\shfolder.dll

Opens key: HKLM\software\microsoft\office\10.0\common\installroot

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

options\msctf.dll

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

Opens kev: 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\psapi.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion Opens kev: HKCU\software\microsoft\internet explorer\settings Opens key: HKLM\software\microsoft\pchealth\errorreporting\dw\debug

HKLM\software\policies\microsoft\pchealth\errorreporting\dw Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dwwin.exe\rpcthreadpoolthrottle HKCU\software\microsoft\windows\currentversion\internet settings Opens key: Opens key: HKLM\software\policies Opens key: HKCU\software\policies Opens key: HKCU\software Opens key: HKLM\software Opens key: HKLM\software\policies\microsoft\internet explorer HKLM\software\policies\microsoft\internet explorer\main Opens key: Opens kev: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content HKI M\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\content Opens key:  $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ settings\5.0\cache\cookies Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\cache\history Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache\history HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\extensible cache  $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Opens kev: settings\5.0\cache\extensible cache\domstore HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\cache\extensible cache\feedplat HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\extensible cache\iecompat  $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Opens key: settings\5.0\cache\extensible cache\ietld HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\cache\extensible cache\mshist012014033120140407 HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\extensible cache\mshist012014041220140413 Opens key:  $\label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\$ settings\5.0\cache\extensible cache\privacie: HKCU\software\microsoft\internet Opens kev: 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 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_skip\_post\_retry\_on\_internetwritefile\_kb895954 Opens key:  $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:local_hammon} soft \end{tabular} windows \current version \current versi$ settings\5.0\cache Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\5.0\cache HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_fix\_chunked\_proxy\_script\_download\_kb843289 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_fix\_chunked\_proxy\_script\_download\_kb843289 HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_use\_cname\_for\_spn\_kb911149 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_use\_cname\_for\_spn\_kb911149 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_use\_spn\_for\_ntlm\_auth\_disabled Opens key: HKLM\software\microsoft\internet  $\verb|explorer\main\featurecontrol\feature\_use\_spn\_for\_ntlm\_auth\_disabled| \\$ Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_allow\_long\_international\_filenames Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_allow\_long\_international\_filenames Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_permit\_cache\_for\_authenticated\_ftp\_kb910274 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_permit\_cache\_for\_authenticated\_ftp\_kb910274 HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_disable\_unicode\_handle\_closing\_callback Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_disable\_unicode\_handle\_closing\_callback

HKCU\software\microsoft\internet

Opens key:

explorer\main\featurecontrol\feature\_disallow\_null\_in\_response\_headers HKLM\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature\_disallow\_null\_in\_response\_headers Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_digest\_no\_extras\_in\_uri Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_digest\_no\_extras\_in\_uri Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_enable\_passport\_session\_store\_kb948608 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_passport\_check\_302\_for\_success\_kb949059 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_passport\_check\_302\_for\_success\_kb949059 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ws2help.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ws2\_32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dwintl.dll HKLM\system\currentcontrolset\services\winsock2\parameters Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\00000004 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000001 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000000 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000003 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000004 Opens kev: Opens kev: Opens key: Opens key: Opens kev: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000010 Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\00000004 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001 Opens kev: Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_return\_failed\_connect\_content\_kb942615 Opens kev: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_return\_failed\_connect\_content\_kb942615 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasman.dll Opens key:  $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$ options\rtutils.dll Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution options\tapi32.dll HKLM\software\microsoft\windows\currentversion\telephony Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasapi32.dll Opens key: HKLM\software\microsoft\tracing\rasapi32 Opens kev: HKLM\software\microsoft\windows nt\currentversion\profilelist Opens key: HKLM\system\currentcontrolset\control\session manager\environment Opens key: Opens key:  $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the current version \end{tabular} profile list \end{tabular} is the current version \end{tabular} and the current version \end{tab$ 1757981266-507921405-1957994488-1003

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

```
options\sensapi.dll
```

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

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

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

Opens key:  $HKLM \ system \ current control \ lsa \ spicache \ msaps spc. dll$ Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll HKLM\svstem\currentcontrolset\control\lsa\sspicache\msnsspc.dll Opens key: Opens key: HKLM\system\currentcontrolset\control\securityproviders\saslprofiles Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\iphlpapi.dll

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

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

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

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

 $options \verb|\msv1_0.dll|$ 

Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat] Oueries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]

Oueries value:

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

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

nt\currentversion\compatibility32[f0da8593d29e9b367fda7028db12cab0]

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

compatibility[f0da8593d29e9b367fda7028db12cab0]

Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit\_dlls] Oueries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]

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

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips] HKLM\software\microsoft\windows\currentversion\explorer\shell Oueries value:

folders[common appdata]

Queries value: HKLM\software\microsoft\windows nt\currentversion\aedebug[auto] HKLM\software\microsoft\windows nt\currentversion\aedebug[debugger] Oueries value:

HKLM\software\microsoft\windows Queries value: nt\currentversion\winlogon[userenvdebuglevel]

HKLM\software\microsoft\windows Oueries value:

nt\currentversion\winlogon[chkaccdebuglevel]

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

folders[personal]

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

folders[local settings]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\winlogon[rsopdebuglevel]

 $\label{thm:logon} \verb+HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]+ on the logon of the logon o$ Queries value:

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

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

Oueries value:

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

Oueries value:

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

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

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

HKLM\system\currentcontrolset\control\computername\activecomputername[computername] HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[domain] Oueries value: Queries value: HKLM\software\microsoft\pchealth\errorreporting[doreport] Oueries value: HKLM\software\microsoft\pchealth\errorreporting[showui] Queries value: HKLM\software\microsoft\pchealth\errorreporting[allornone]

Queries value: HKLM\software\microsoft\pchealth\errorreporting[includemicrosoftapps] Oueries value: HKLM\software\microsoft\pchealth\errorreporting[includewindowsapps]

HKLM\software\microsoft\pchealth\errorreporting[dotextlog] Oueries value:

Oueries value: HKLM\software\microsoft\pchealth\errorreporting[includekernelfaults] Oueries value: HKLM\software\microsoft\pchealth\errorreporting[includeshutdownerrs] Queries value: HKLM\software\microsoft\pchealth\errorreporting[numberoffaultpipes] Oueries value: HKLM\software\microsoft\pchealth\errorreporting[numberofhangpipes] Queries value: HKLM\software\microsoft\pchealth\errorreporting[maxuserqueuesize] HKLM\software\microsoft\pchealth\errorreporting[forcequeuemode] Oueries value:

Oueries value:

Queries value: HKLM\software\microsoft\rpc[maxrpcsize] Oueries value: HKLM\system\currentcontrolset\control\session

manager[safeprocesssearchmode]

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

manager\appcompatibility[disableappcompat]

Queries value: HKLM\system\wpa\mediacenter[installed]

Queries value:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [authenticode enabled]$ 

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

Queries value:

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

Oueries value:

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

Queries value:

Queries value:

Queries value:

Queries value:

Queries value:

Queries value:

Oueries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{7fb9cd2e-3076-4df9-a57b-b813f72dbb91\} [itemsize]$ 

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{7fb9cd2e-3076-4df9-a57b-b813f72dbb91\} \ [saferflags]$ 

Queries 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}\[saferflags\]$ 

Queries value:

Queries value:

Queries value:

 $HKLM \ software \ blicies \ icrosoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{94e3e076-8f53-42a5-8411-085bcc18a68d\} [itemsize]$ 

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{94e3e076-8f53-42a5-8411-085bcc18a68d\} \ [saferflags]$ 

Queries value:

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

Oueries value:

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

Queries value:

Queries value:

 $HKLM\software\policies\mbox{$dc971ee5-44eb-4fe4-ae2e-b91490411bfc} [saferflags] \\$ 

Queries value:

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

Queries value:

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

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

folders[cache]
Queries value:

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

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

Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[dwwin]

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

```
compatibility[dwwin]
                          HKLM\system\currentcontrolset\control\session
 Oueries value:
manager[criticalsectiontimeout]
 Queries value:
                          HKLM\software\microsoft\ole[rwlockresourcetimeout]
 Oueries value:
                          HKCR\interface[interfacehelperdisableall]
 Queries value:
                          HKCR\interface[interfacehelperdisableallforole32]
 Oueries value:
                          HKCR\interface[interfacehelperdisabletypelib]
                          HKCR\interface\{00020400-0000-0000-c000-
 Oueries value:
00000000046}[interfacehelperdisableall]
                          HKCR\interface\{00020400-0000-0000-c000-
 Oueries value:
00000000046}[interfacehelperdisableallforole32]
 Queries value:
                          \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
settings[disableimprovedzonecheck]
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[dwwin.exe]
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
 Queries value:
                          HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
ab78-1084642581fb1
                          Oueries value:
0000-0000000000000]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
 Oueries value:
 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:
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
 Queries value:
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
 Queries value:
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
 Queries value:
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
 Oueries value:
                          HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [aux 5]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
 Oueries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
 Queries value:
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
 Oueries value:
                          HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [mixer 8]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
 Queries value:
                          HKCU\software\microsoft\multimedia\audio[systemformats]
 Oueries value:
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.imaadpcm]
 Queries value:
HKLM \verb|\software\m| icrosoft\audiocompression manager\driver cache \verb|\m| sacm.imaadpcm[fdwsupport]|
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[aformattagcache]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cfiltertags]
                          HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\drivers32[msacm.msadpcm]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[fdwsupport]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cformattags]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[aformattagcache]
```

Queries value:

```
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cfiltertags]
                          HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\drivers32[msacm.msg711]
 Queries value:
HKLM \verb|\software\microsoft| audio compression manager \verb|\drivercache\msacm.msg711[fdwsupport]| \\
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cformattags]
 Oueries value:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msg711[aformattag cache]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cfiltertags]
                           HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\drivers32[msacm.msgsm610]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[fdwsupport]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cformattags]
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msgsm610 [a formattag cache]
 Queries value:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. msgsm610[cfilter tags]
                           HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\drivers32[msacm.trspch]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport]
 Queries value:
HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus msacm.trspch[cformattags]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cfiltertags]
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msg723]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[fdwsupport]
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cformattags]
 Queries value:
HKLM \backslash software \backslash microsoft \backslash audio compression manager \backslash driver cache \backslash msacm. msg723 [a formattag cache]
 Queries value:
HKLM \verb|\software\microsoft\audiocompressionmanager\drivercache\mbox{|} msg723[cfiltertags]|
                          HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msaudio1]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[fdwsupport]
 Queries value:
HKLM \verb| software \verb| microsoft \verb| audiocompression manager \verb| driver cache \verb| msaudio1[cformattags]| \\
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[aformattagcache]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cfiltertags]
                          HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\drivers32[msacm.sl_anet]
 Queries value:
HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus msacm. sl\_anet[fdwsupport]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cformattags]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[aformattagcache]
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl anet[cfiltertags]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2\fdwsupport1
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cformattags]
 Queries value:
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cfiltertags]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.l3acm]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[fdwsupport]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cformattags]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[aformattagcache]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags]
                          HKCU\software\microsoft\multimedia\audio compression
 Oueries value:
manager\msacm[nopcmconverter]
                          HKCU\software\microsoft\multimedia\audio compression manager\priority
 Oueries value:
v4.00[priority1]
```

```
Oueries value:
                           HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
                           HKCU\control panel\desktop[lamebuttontext]
  Oueries value:
  Oueries value:
                           HKLM\software\microsoft\windows\currentversion[programfilesdir]
                           HKLM\software\microsoft\windows\currentversion[commonfilesdir]
  Queries value:
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
  Oueries value:
                           HKLM\software\microsoft\ctf\systemshared[cuas]
  Oueries value:
                           HKCU\keyboard layout\toggle[language hotkey]
  Oueries value:
                           HKCU\keyboard layout\toggle[hotkey]
  Oueries value:
                           HKCU\keyboard layout\toggle[layout hotkey]
                           HKLM\software\microsoft\ctf[enableanchorcontext]
  Oueries value:
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion[digitalproductid]
  Oueries value:
                           HKCU\software\microsoft\internet explorer\settings[anchor color]
                           HKLM\software\microsoft\pchealth\errorreporting\dw[buildpipemachine]
  Oueries value:
  Queries value:
                           HKLM\software\microsoft\pchealth\errorreporting\dw[dwfiletreeroot]
  Queries value:
                           HKLM\software\microsoft\pchealth\errorreporting\dw[dwtracking]
                           HKLM\software\microsoft\pchealth\errorreporting\dw[dwnoexternalurl]
  Oueries value:
  Queries value:
                           HKLM\software\microsoft\pchealth\errorreporting\dw[dwnofilecollection]
  Queries value:
HKLM \setminus software \setminus microsoft \setminus pchealth \setminus error reporting \setminus dw[dwnosecondlevel collection]
                           HKLM\software\microsoft\pchealth\errorreporting\dw[dwurllaunch]
  Queries value:
  Queries value:
                           HKLM\software\microsoft\pchealth\errorreporting\dw[dwneverupload]
                           HKLM\software\microsoft\pchealth\errorreporting\dw[dwreporteename]
  Queries value:
  Queries value:
                           HKLM\software\microsoft\pchealth\errorreporting\dw[dwnocollectionlink]
  Queries value:
                           HKLM\software\microsoft\pchealth\errorreporting\dw[dwallowheadless]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[secureprotocols]
                           HKLM\software\policies\microsoft\internet
  Queries value:
explorer\main[security_hklm_only]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[certificaterevocation]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablepassport]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
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:
                           HKCU\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:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
                           \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
  Oueries value:
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache[signature]
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings\5.0\cache\content[peruseritem]
                           HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\content[peruseritem]
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Oueries value:
folders[cache]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\content[cachelimit]
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
  Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cachelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\history[peruseritem]
```

```
Oueries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\history[cacheprefix]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
settings\5.0\cache\extensible cache\domstore[cacherepair]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
                            \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
 Queries value:
settings\5.0\cache\extensible cache\domstore[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cacherepair]
                            \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacherepair]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\ietld[cacherepair]
 Queries value:
                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings\5.0\cache\extensible cache\ietld[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\ietld[cacheprefix]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings\5.0\cache\extensible cache\ietld[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\extensible cache\privacie:[cacherepair]
 Queries value:
                            settings\5.0\cache\extensible cache\privacie:[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\extensible cache\privacie:[cachelimit]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disableworkerthreadhibernation]
 Queries value:
                            \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
settings[disableworkerthreadhibernation]
```

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

Queries value:

```
settings[disablereadrange]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[socketsendbufferlength]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
 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[keepalivetimeout]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
 Queries value:
                            \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
settings[maxconnectionsperserver]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsper1_0server]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[serverinfotimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connecttimeout]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connecttimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connectretries]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connectretries]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendtimeout]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendtimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[receivetimeout]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[receivetimeout]
 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[disablentlmpreauth]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[scavengecachelowerbound]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[certcachenovalidate]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[ftpdefaultexpirytimesecs]
 Queries value:
                            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[dwwin.exe]
 Queries value:
                            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
                            \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[disablecachingofsslpages]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[perusercookies]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablent4rascheck]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dialupuselansettings]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[bvpassftptimecheck]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduringauth]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[releasesocketduring401auth]
 Oueries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablelegacypreauthasserver]
```

```
Oueries value:
                         HKLM\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
 Queries value:
                         \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
settings[bypasshttpnocachecheck]
                         HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasshttpnocachecheck]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasssslnocachecheck]
                         HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasssslnocachecheck]
                         HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablehttptrace]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[nocheckautodialoverride]
                         HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[nocheckautodialoverride]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dontusednsloadbalancing]
                         HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dontusednsloadbalancing]
                         HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sharecredswithwinhttp]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
                         \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings[headerexclusionlistforcache]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dnscacheenabled]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dnscacheentries]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dnscachetimeout]
                         \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings[warnonpost]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
                         \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Oueries value:
settings[warnonzonecrossing]
                         \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings[warnonbadcertsending]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonpostredirect]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9[serial access num]
 Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
 Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000004[packedcatalogitem]
 Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 0000000000005 \ [packed catalog item]
 Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 0000000000006 \ [packed catalog item]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Queries value:
```

```
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ (catalog\_entries \ 00000000001[library path])
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap amespace\_catalog \\ S \setminus catalog\_entries \setminus 000000000001[providerid]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000001[supported name space]]
 Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog 5 \setminus catalog\_entries \setminus 000000000001[storesserviceclass info]
 Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ (catalog\_entries \ 000000000002[library path])
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
 Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ set alog\_entries \ (0000000000002 \ [version])
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000002[storesserviceclassinfo]
 Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ (catalog\_entries \ 00000000003 \ [library path]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[globaluseroffline]
 Queries value:
                       \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
settings[enableautodial]
 Queries value:
                       HKLM\software\microsoft\windows\currentversion\internet
settings[urlencoding]
 Oueries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings[truncatefilename]
                       HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[badproxyexpirestime]
 Queries value:
HKLM \ software \ microsoft \ windows \ current version \ telephony \ [tapi32max numrequestretries]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32requestretrytimeout]
                       HKLM\software\microsoft\tracing[enableconsoletracing]
 Oueries value:
 Queries value:
                       HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
 Oueries value:
                       HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
 Queries value:
                       HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
 Oueries value:
                       HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
 Queries value:
                       HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
                       HKLM\software\microsoft\tracing\rasapi32[filedirectory]
 Oueries value:
                       HKLM\software\microsoft\windows\currentversion\explorer\user shell
 Oueries value:
folders[common appdata]
 Queries value:
                       HKLM\software\microsoft\windows
nt\currentversion\profilelist[profilesdirectory]
 Queries value:
                       HKLM\software\microsoft\windows
nt\currentversion\profilelist[allusersprofile]
 Oueries value:
                       HKLM\software\microsoft\windows
nt\currentversion\profilelist[defaultuserprofile]
 Queries value:
                       HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
```

1757981266-507921405-1957994488-1003[profileimagepath]

HKCU\software\microsoft\windows

Queries value:

```
nt\currentversion\winlogon[parseautoexec]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
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:
                          \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
settings\connections[savedlegacysettings]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\connections[defaultconnectionsettings]
 Queries value:
                          HKCU\software\microsoft\windows nt\currentversion\windows[scrollinset]
                          HKCU\software\microsoft\windows nt\currentversion\windows[dragde]avl
 Oueries value:
 Queries value:
                          HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]
 Queries value:
                          HKCU\software\microsoft\windows nt\currentversion\windows[scrolldelay]
 Oueries value:
                          HKCU\software\microsoft\windows
nt\currentversion\windows[scrollinterval]
                          HKLM\software\microsoft\rpc\securityservice[10]
 Queries value:
 Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
 Queries value:
                          HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
 Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]
 Queries value:
HKLM \setminus system \setminus current control \\ \  \mid sansspic a che \setminus msaps spc. \\ dll[capabilities]
                          HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]
 Queries value:
 Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[version]
                          HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]
 Queries value:
 Queries value:
HKLM \setminus system \setminus current control \setminus lsa \setminus sspicache \setminus msaps spc.dll[token size]
 Queries value:
                          HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]
 Queries value:
                          HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]
 Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities]
 Queries value:
                          HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid]
                          HKLM\system\currentcontrol\set\control\lsa\sspicache\digest.dll[version]
 Oueries value:
                          HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]
 Queries value:
 Oueries 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]
 Oueries 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[type]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize]
                          HKLM\software\microsoft\cryptography\rng[seed]
 Value changes:
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[appdata]
                          HKCU\software\microsoft\windows\currentversion\explorer\shell
 Value changes:
folders[personal]
                          HKCU\software\microsoft\windows\currentversion\explorer\shell
 Value changes:
folders[cache]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cookies]
 Value changes:
                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ shell
folders[history]
 Value changes:
```

 $\label{lem:hklm} \verb+Kklm\+ software\+ icrosoft\+ windows\+ current version\+ explorer\+ shell$ 

folders[common appdata]

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

settings[proxyenable]

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

settings\connections[savedlegacysettings]