Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 622, Task ID: 2434

Task ID: 2434

Risk Level: 8

Date Processed: 2016-02-22 05:29:43 (UTC)

Processing Time: 61.2 seconds
Virtual Environment: IntelliVM

Execution Arguments:

"c:\windows\temp\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe"

Sample ID: 622 Type: basic Owner: admin

Label: 33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99

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

File Type: PE32:win32:gui File Size: 54272 bytes

MD5: 75984f5cee7f9e64b9ffe44f60df8764

SHA256: 33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99

Description: None

Pattern Matching Results

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

4 Reads process memory

6 Contacts service to find external IP address

8 Starts svchost.exe

Writes to memory of system processes

Process/Thread Events

Creates process:

 $\begin{tabular}{ll} C: \WINDOWS\Temp\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe \\ \begin{tabular}{ll} C: \WINDOWS\Temp\33a18d17f6f150459e8eb2593a364b55868a1c85f4ee897aed2b83e30cefe9$

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

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

Reads from process: PID:244 C:\WINDOWS\system32\svchost.exe
Writes to process: PID:244 C:\WINDOWS\system32\svchost.exe

Terminates process:

C:\WINDOWS\Temp\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe

Named Object Events

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

1957994488-1003 Creates mutex:

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

1957994488-1003

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

1957994488-1003

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

1957994488-1003

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

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

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

Creates mutex: \BaseNamedObjects\SHIMLIB_LOG_MUTEX

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

settings!temporary internet files!content.ie5!

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

settings!history!history.ie5!

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

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

 $\label{lem:continuous} $$\operatorname{Semaphore}: $$ \aseNamedObjects\sell. \{A48F1A32-A340-11D1-BC6B-00A0C90312E1\} $$ \aseNamedObjects\sell. \{210A4BA0-3AEA-1069-A2D9-08002B30309D\} $$ \aseNamedObjects\sell. \{210A4BA0-2AEA-1069-A2D9-08002B30309D\} $$ \aseNamedObjects\sell. \{210A4BA0-2AEA-1069-A2D9-0800$

File System Events

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

Files\Content.IE5\QXMNQBKF\icanhazip_com[1].txt

Opens: C:\WINDOWS\Prefetch\33A18D17F6F150459E8EB2593A364-3910D469.pf

Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\system32\imm32.dl1
Opens: C:\WINDOWS\system32\comctl32.dl1

Opens: C:\WINDOWS\system32\COMCTL32.dll.124.Manifest
Opens: C:\WINDOWS\system32\COMCTL32.dll.124.Config

Opens: C:\WINDOWS\system32\MSCTF.dll

```
C:\WINDOWS\system32\MSCTFIME.IME
 Opens:
 Opens:
                         C:\WINDOWS\system32\ole32.dll
 Opens:
                         C:\WINDOWS\system32\svchost.exe
 Opens:
                         C:\WINDOWS\system32\apphelp.dll
 Opens:
                         C:\WINDOWS\AppPatch\sysmain.sdb
 Opens:
                         C:\WINDOWS\AppPatch\systest.sdb
 Opens:
                         C:\WINDOWS\system32
 Opens:
                         C:\
                         C:\WTNDOWS
 Opens:
 Opens:
                         C:\WINDOWS\system32\svchost.exe.Manifest
 Opens:
                         C:\WINDOWS\Prefetch\SVCHOST.EXE-3530F672.pf
 Opens:
                         C:\WINDOWS\system32\shimeng.dll
 Opens:
                         C:\WINDOWS\AppPatch\AcGenral.dll
                         C:\WINDOWS\system32\winmm.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\msacm32.dll
                         C:\WINDOWS\system32\uxtheme.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\shell32.dll
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Config
 Opens:
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
 Opens:
                         C:\WINDOWS\WindowsShell.Manifest
 Opens:
                         C:\WINDOWS\WindowsShell.Config
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Config
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Manifest
                         C:\WINDOWS\system32\urlmon.dll.123.Config
 Opens:
 Opens:
                         C:\WINDOWS\system32\wininet.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\wininet.dll.123.Config
 Opens:
C:\WINDOWS\Temp\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe
 Opens:
                         C:\WINDOWS\Temp\5277c511-40ed-4b65-8746-20554de913a0
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5
                         C:\Documents and Settings\Admin\Local Settings\History
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History\History.IE5
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Cookies
 Opens:
                         C:\Documents and Settings\Admin\Cookies\index.dat
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\index.dat
 Opens:
                         C:\WINDOWS\system32\ws2_32.dll
                         C:\WINDOWS\system32\ws2help.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\rasapi32.dll
 Opens:
                         C:\WINDOWS\system32\rasman.dll
                         C:\WINDOWS\system32\netapi32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\tapi32.dll
 Opens:
                         C:\WINDOWS\system32\rtutils.dll
                         C:\WINDOWS\system32\TAPI32.dll.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\TAPI32.dll.124.Config
 Opens:
                         C:\AUTOEXEC.BAT
                         C:\Documents and Settings\All Users\Application
 Opens:
Data\Microsoft\Network\Connections\Pbk
                         C:\WINDOWS\system32\ras
 Opens:
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Microsoft\Network\Connections\Pbk\
 Opens:
                         C:\WINDOWS\system32\sensapi.dll
                         C:\WINDOWS\system32\mswsock.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\rasadhlp.dll
 Opens:
                         C:\WINDOWS\system32\dnsapi.dll
 Opens:
                         C:\WINDOWS\system32\iphlpapi.dll
 Opens:
                         C:\WINDOWS\system32\drivers\etc\hosts
 Opens:
                         C:\WINDOWS\system32\rsaenh.dll
                         C:\WINDOWS\system32\msv1_0.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\crypt32.dll
 Opens:
                         C:\WINDOWS\system32\hnetcfg.dll
                         C:\WINDOWS\system32\wshtcpip.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\msasn1.dll
 Opens:
                         C:\Documents and Settings\Admin\Application
{\tt Data\Microsoft\System\Certificates\My\Certificates}
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My\CRLs
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My\CTLs
 Opens:
                         C:\WINDOWS\system32\wintrust.dll
 Opens:
                         C:\WINDOWS\system32\schannel.dll
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\icanhazip_com[1].txt
 Reads from:
                         C:\AUTOEXEC.BAT
```

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

Deletes:

C:\WINDOWS\Temp\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe

Network Events

DNS query: icanhazip.com

DNS response: icanhazip.com ⇒ 64.182.208.181

Connects to: 64.182.208.181:80 Connects to: 197.149.90.166:12232 Connects to: 173.216.247.74:443 Connects to: 77.48.30.156:443

Sends data to: 8.8.8.8:53

icanhazip.com:80 (64.182.208.181) Sends data to:

Receives data from: 0.0.0.0:0

Receives data from: icanhazip.com:80 (64.182.208.181)

Windows Registry Events

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

Creates key: HKCU\software\microsoft\multimedia\audio compression manager\ Creates key: $\label{lem:hkcu} \mbox{HKCU\software\mbox{\sc multimedia\audio compression manager\sc manager\sc$ Creates key: HKCU\software\microsoft\multimedia\audio compression manager\priority

v4.00

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

folders

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

Creates key: HKLM\software\microsoft\tracing

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

folders

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

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

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

settings\connections

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

awareness

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

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

options\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe

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

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

options\gdi32.dll

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

options\user32.dll

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

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

options\kernel32.dll

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

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

Opens key:

options\secur32.dll

Opens key:

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

Opens key: options\advapi32.dll

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

Opens key:

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

options\comctl32.dll Opens key:

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

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

Opens key:

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

Opens key: HKCU\

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

HKCU\control panel\desktop Opens key:

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

options\msvcrt.dll

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

options\msctf.dll

Opens key:

 $HKLM \setminus software \setminus microsoft \setminus ctf \setminus compatibility \setminus 33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe$

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

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

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

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

options\version.dll

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

options\msctfime.ime

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

options\ole32.dll

Opens key: HKLM\software\microsoft\ole

Opens key: HKCR\interface

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

Opens key: HKCU\software\microsoft\ctf

 ${\it HKLM \ } software \ \\ microsoft \ \\ ctf \ \\ systems hared$ Opens key:

Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\apphelp.dll

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers

Opens key: HKLM\software\microsoft\windows

 $\verb|nt\currentversion\appcompatflags\custom\svchost.exe|$ Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags Opens key: HKLM\software\policies\microsoft\windows\safer\levelobjects

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

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-

be2efd2c1a33}

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

Opens key:

edd5fbde1328}

Opens key:

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

Opens key:

7c29ddecae3f}

Opens key:

085bcc18a68d}

Opens key:

b91490411bfc} Opens key:

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

Opens kev:

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: $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus paths$

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones

Opens key:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus paths$ Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones

Opens kev:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones

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\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
  Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
  Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\explorer\shell folders
                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\svchost.exe
                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\acgenral.dll
  Opens key:
                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shimeng.dll
  Opens key:
                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winmm.dll
                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\oleaut32.dll
  Opens key:
                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msacm32.dll
  Opens kev:
                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shlwapi.dll
                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\shell32.dll
  Opens key:
                                       \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution
options\userenv.dll
  Opens kev:
                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
                                       HKLM\software\microsoft\windows nt\currentversion\drivers32
  Opens kev:
  Opens key:
Opens key:
                                       HKLM\software\microsoft\oleaut
                                       HKLM\software\microsoft\oleaut\userera
  Opens kev:
  Opens key:
                                       HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache
  Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm
  Opens key:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. msadpcm
                                       HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711
  Opens kev:
  Opens key:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. \ msgsm610
                                       HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch
  Opens kev:
  Opens key:
                                       HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723
  Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1
  Opens key:
\label{thm:local_hammon} \begin{tabular}{ll} HKLM \label{thm:local_hammon} soft \label{thm:local_hammon} an ager \label{thm:local_hammon} \end{tabular} an et it is a constant. The third is a constant in the local hammon hamm
  Opens kev:
                                       HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2
  Opens key:
                                       HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. 13 acm
  Opens key:
                                       HKLM\system\currentcontrolset\control\mediaresources\acm
  Opens key:
                                       HKLM\software\microsoft\windows\currentversion\explorer\performance
  Opens key:
                                       HKLM\system\setup
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:
                                       \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\advanced}} \mbox{\tt advanced}
  Opens key:
                                       HKLM\software\microsoft\windows nt\currentversion\languagepack
  Opens key:
                                       HKLM\system\currentcontrolset\control\productoptions
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Opens kev:
                                       HKLM\software\policies\microsoft\windows\system
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\thememanager
                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\normaliz.dll
  Opens key:
                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iertutil.dll
  Opens key:
                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\urlmon.dll
```

```
HKCU\software\classes\
  Opens key:
  Opens key:
                                      HKCU\software\classes\protocols\name-space handler\
  Opens kev:
                                      HKCR\protocols\name-space handler
                                      HKCU\software\classes\protocols\name-space handler
  Opens key:
  Opens key:
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:
                                      HKLM\software\microsoft\windows\currentversion\internet settings
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
  Opens key:
                                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\
  Opens key:
                                      HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
                                      HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens kev:
  Opens key:
                                      HKLM\software\microsoft\internet explorer\main\featurecontrol
  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
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zonemap\domains\
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zonemap\ranges\
  Opens key:
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
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\software\microsoft\windows nt\currentversion\image file execution
options\wininet.dll
                                      HKLM\system\currentcontrolset\control\wmi\security
  Opens key:
  Opens key:
                                      HKLM\system\currentcontrolset\control\computername
  Opens key:
                                      HKLM\system\currentcontrolset\control\computername\activecomputername
                                      \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearings}} \ \ \mbox{\tt microsoft\windows\currentversion\linearings}} \ \mbox{\tt microsoft\windows\currentversion\linearings}} \ \ \mbox{\tt microsoft\windows\currentversion\linearings}} \ \mbox{\tt microsoft\windows\currentversion\windows\currentversion\linearings}} \ \mbox{\tt microsoft\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\windows\windows\windows\currentversion\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows
  Opens key:
  Opens key:
                                      HKLM\software\policies
  Opens key:
                                      HKCU\software\policies
                                      HKCU\software
  Opens key:
  Opens key:
                                      HKLM\software
  Opens key:
                                      HKLM\software\policies\microsoft\internet explorer
                                      HKLM\software\policies\microsoft\internet explorer\main
  Opens key:
  Opens key:
                                      HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\5.0\cache\content
                                      HKLM\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\content
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
                                      HKLM\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\cookies
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
  Opens key:
                                      HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
  Opens key:
                                      HKLM\software\microsoft\rpc\pagedbuffers
  Opens key:
                                      HKLM\software\microsoft\rpc
  Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\svchost.exe\rpcthreadpoolthrottle
                                      HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:
  Opens key:
                                      \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings\5.0\cache\extensible cache
                                      \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}.
  Opens key:
settings\5.0\cache\extensible cache\domstore
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\extensible cache\mshist012014033120140407
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413
  Opens key:
                                      \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
```

```
Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
 Opens key:
                       HKLM\software\microsoft\internet
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:
                       HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
 Opens key:
                       HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                       HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                       HKCU\software\microsoft\internet
 Opens key:
explorer \verb|\main\featurecontrol\feature\_use\_cname\_for\_spn\_kb911149
 Opens key:
                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
 Opens key:
                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
                       HKLM\software\microsoft\internet
 Opens key:
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 \verb|\main| featurecontrol| feature_permit_cache_for_authenticated_ftp\_kb910274
                       HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens key:
                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
                      HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
                       HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 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
                       HKLM\system\currentcontrolset\services\winsock2\parameters
 Opens key:
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
 Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
 Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
```

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ parameters \ protocol_catalog_entries \ protocol_catalog \ parameters \ parameters$

settings\5.0\cache\extensible cache\privacie:

Opens key:

Opens key:

```
Opens key:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog9 \ catalog\_entries \ 000000000010
  Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ (catalog\_entries \ 0000000000011) \ (catalog\_entries \ (catalog \ (catalog\_entries \ (catalog \ (cata
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
  Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000
  Opens key:
HKCU\software\microsoft\windows\currentversion\internet settings\wpad
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens kev:
                                    HKCU\software\microsoft\windows\currentversion\internet settings\http
filters\rpa
  Opens key:
                                    HKLM\software\microsoft\windows\currentversion\internet settings\http
filters\rpa
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
                                    HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_mime_handling
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_mime_handling
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netapi32.dll
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasman.dll
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\rtutils.dll
  Opens key:
                                    \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution
options\tapi32.dll
  Opens kev:
                                    HKLM\software\microsoft\windows\currentversion\telephonv
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasapi32.dll
                                    HKLM\software\microsoft\tracing\rasapi32
  Opens key:
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\profilelist
  Opens key:
                                    HKLM\system\currentcontrolset\control\session manager\environment
                                    HKLM\software\microsoft\windows\currentversion
  Opens kev:
  Opens key:
                                    HKU\
                                    HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
  Opens key:
1757981266-507921405-1957994488-1003
  Opens key:
                                    HKCU\environment
  Opens key:
                                    HKCU\volatile environment
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\sensapi.dll
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mswsock.dll
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\rasadhlp.dll
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_http_username_password_disable
  Opens key:
                                    \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings\zonemap\
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
  Opens key:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\protocoldefaults\
  Opens key:
                                    \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings\zonemap\domains\
  Opens key:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\msn.com
  Opens key:
                                    \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
settings\zonemap\domains\msn.com\related
```

HKCU\software\microsoft\internet

Opens key:

```
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
                          HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
                          HKCU\software\microsoft\internet explorer\ietld
 Opens key:
 Opens key:
                          HKLM\software\policies\microsoft\internet explorer\security
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
 Opens key:
                          \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\zones\
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
                          \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
 Opens key:
settings\zones\1
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\2
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\3
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\4
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
                          HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
                          HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecon
                         trol\feature_localmachine_lockdown
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\0
 Opens key:
                          \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\0
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\1
 Opens key:
                          \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\1
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\2
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\2
                          \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
 Opens key:
settings\lockdown_zones\2
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\3
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\3
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\4
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\4
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
                          HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dnsapi.dll
                          HKLM\system\currentcontrolset\services\dnscache\parameters
 Opens key:
 Opens key:
                          HKLM\software\policies\microsoft\windows nt\dnsclient
```

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

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:

c7d49d7cecdc}

Opens key: ${\tt HKLM \setminus software \setminus policies \setminus microsoft \setminus system \setminus dnsclient}$

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

cryptographic provider

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

Opens key: HKLM\system\currentcontrol\securityproviders
Opens key: HKLM\system\currentcontrol\set\control\lsa\sspicache

Opens key: HKLM\system\currentcontrol\sa\sspicache\msapsspc.dll
Opens key: HKLM\system\currentcontrol\sa\sspicache\digest.dll
Opens key: HKLM\system\currentcontrol\sa\sspicache\msnsspc.dll
Opens key: HKLM\system\currentcontrol\set\control\sa\sspicache\msnsspc.dll
Opens key: HKLM\system\currentcontrol\set\control\securityproviders\saslprofiles
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msv1_0.dll

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

options\rsaenh.dll

 $Opens\ key: \\ \hspace{1.5cm} \text{HKLM} \\ software \\ \text{microsoft} \\ cryptography \\ offload$

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

options\hnetcfg.dll

Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\wshtcpip.dll

Opens key: HKCU\software\classes\mime\database\content type\text/plain;

charset=utf-8

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

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

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

options\msasn1.dll

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

options\crypt32.dll

Opens key: ${\tt HKLM \backslash software \backslash microsoft \backslash cryptography \backslash oid}$

 $\label{lem:condition} Opens~key: $$ HKLM\software\microsoft\cryptography\oid\encodingtype 0 $$ Opens~key: $$ HKLM\software\microsoft\cryptography\oid\encodingtype $$ $$$

0\certdllopenstoreprov

Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype

0\certdllopenstoreprov\#16

Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype

0\certdllopenstoreprov\ldap

Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype

1\certdllopenstoreprov

Opens key: HKCU\software\microsoft\systemcertificates\my\physicalstores

Opens key: HKCU\software\microsoft\systemcertificates\my
Opens key: HKCU\software\microsoft\systemcertificates\my\

Opens key: HKCU\software\microsoft\systemcertificates\my\certificates
Opens key: HKCU\software\microsoft\systemcertificates\my\crls
Opens key: HKCU\software\microsoft\systemcertificates\my\ctls

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

options\imagehlp.dll

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

options\wintrust.dll

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

options\schannel.dll

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

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

Queries value:

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

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

nt\currentversion\compatibility32[33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99]

Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99]

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

Queries value: HKCU\control panel\desktop[multiuilanguageid]
Queries value: HKCU\control panel\desktop[smoothscroll]
Queries value: HKLM\software\microsoft\ctf\systemshared[cuas]

Oueries value: HKCU\keyboard layout\toggle[language hotkey] HKCU\keyboard layout\toggle[hotkey] Oueries value: Oueries value: HKCU\keyboard layout\toggle[layout hotkey] HKLM\software\microsoft\ctf[enableanchorcontext] Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file] Oueries value: Queries value: HKLM\system\currentcontrolset\control\session manager[criticalsectiontimeout] HKLM\software\microsoft\ole[rwlockresourcetimeout] Oueries value: Queries value: HKCR\interface[interfacehelperdisableall] Queries value: HKCR\interface[interfacehelperdisableallforole32] Oueries value: HKCR\interface[interfacehelperdisabletypelib] Queries value: HKCR\interface\{00020400-0000-0000-c000-00000000046}[interfacehelperdisableall] HKCR\interface\{00020400-0000-0000-c000-Oueries value: 00000000046}[interfacehelperdisableallforole32] Queries value: HKCU\software\microsoft\ctf[disable thread input manager] Queries value: HKLM\system\currentcontrolset\control\session manager[safeprocesssearchmode] HKLM\system\currentcontrolset\control\session Queries value: manager\appcompatibility[disableappcompat] HKLM\system\wpa\mediacenter[installed] Queries value: Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled] HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels] Queries value: Queries value: be2efd2c1a33}[itemdata] Queries value: be2efd2c1a33}[saferflags] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89edd5fbde1328}[itemdata] Queries value: $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{349d35ab-37b5-462f-9b89-4666f-9b89-46666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b8$ edd5fbde1328}[hashalg] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89edd5fbde1328}[itemsize] Queries value: edd5fbde1328}[saferflags] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57bb813f72dbb91}[itemdata] Queries value: $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{7fb9cd2e-3076-4df9-a57b-4df9-a57$ b813f72dbb91}[hashalg] Oueries value:

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

Oueries value:

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

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[itemdata]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[hashalg]

Queries value:

7c29ddecae3f}[itemsize]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[saferflags]

Queries value:

 $HKLM \setminus software \setminus policies \setminus irros oft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes \setminus \{94e3e076-8f53-42a5-8411-4264-8411-4264-8411-4264-8411-4266-8411-4266-8411-4266-8411-4266-8411-4266-841$ 085bcc18a68d}[itemdata]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[hashalg]

Oueries value:

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

Oueries value:

085bcc18a68d}[saferflags]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2eb91490411bfc}[itemdata]

Oueries value:

```
b91490411bfc}[hashalg]
 Oueries value:
b91490411bfc}[itemsize]
 Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[saferflags]
 Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
 Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
 Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\compatibilitv32[svchost]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[svchost]
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
 Queries value:
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
 Queries value:
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
 Queries value:
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
 Queries value:
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
 Queries value:
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
 Queries value:
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
 Oueries value:
                         HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [aux 7]
```

Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9] Oueries value: Queries value: HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer] Queries 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[mixer31 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7] HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]

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

Queries value: HKLM\software\microsoft\windows

nt\currentversion\drivers32[msacm.imaadpcm]

Queries value:

 $\label{lem:hklmsoftware} HKLM \ software \ `microsoft\ audiocompression manager \ driver cache \ `maadpcm[fdw support] \ Oueries \ value:$

WKLMM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags]
Oueries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[aformattagcache]
 Oueries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cfiltertags]
Queries value: HKLM\software\microsoft\windows

nt\currentversion\drivers32[msacm.msadpcm]

Queries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[fdwsupport]
 Queries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cformattags]
Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\audiocompression manager\drivercache\mbox{\sc m.msadpcm[aformattagcache]} \\ Queries\ value:$

```
nt\currentversion\drivers32[msacm.msg711]
   Oueries value:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msg711[fdwsupport]
   Queries value:
HKLM \verb|\software\microsoft\audiocompressionmanager\drivercache\mbox|\mbox| msg711[cformattags]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[aformattagcache]
   Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cfiltertags]
                                                  HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\drivers32[msacm.msgsm610]
   Queries value:
Oueries value:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. msgsm610[cformattags]
   Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[aformattagcache]
   Queries value:
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msgsm610 [cfilter tags]
   Queries value:
                                                  HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.trspch]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport]
HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} which is a constant and in the lemma substitution of t
   Queries value:
Queries value:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.trspch[cfiltertags]
                                                  HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msg723]
   Queries value:
HKLM \verb|\software\microsoft| audio compression manager \verb|\drivercache\msacm.msg723[fdwsupport]| \\
   Queries value:
HKLM \verb|\software\microsoft\audiocompressionmanager\drivercache\mbox{|}msacm.msg723[cformattags]|
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[aformattagcache]
   Oueries value:
HKLM \verb|\software\microsoft| audiocompression manager \verb|\drivercache\msg723[cfiltertags]|
                                                  HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\drivers32[msacm.msaudio1]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[fdwsupport]
   Queries value:
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msaudio1[cformattags]
   Queries value:
HKLM \verb|\software\microsoft\audiocompression| manager \verb|\driver| cache \verb|\msaudio1| [aformattag cache]| and the standard of t
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cfiltertags]
   Queries value:
                                                  HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.sl_anet]
   Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[fdwsupport]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl anet[cformattags]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[aformattagcache]
   Oueries value:
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. sl\_anet [cfilter tags]
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport]
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cformattags]
   Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[aformattagcache]
   Queries value:
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. iac2 [cfilter tags]
   Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.l3acm]
   Oueries value:
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. 13 acm [fdw support]
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cformattags]
   Queries value:
Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags]
   Oueries value:
                                                  HKCU\software\microsoft\multimedia\audio compression
manager\msacm[nopcmconverter]
   Queries value:
                                                  HKCU\software\microsoft\multimedia\audio compression manager\priority
v4.00[priority1]
   Oueries value:
                                                  HKLM\system\setup[systemsetupinprogress]
   Queries value:
```

HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips] HKLM\software\microsoft\windows Oueries value: nt\currentversion\winlogon[userenvdebuglevel] Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[chkaccdebuglevel] Queries value: HKLM\system\currentcontrolset\control\productoptions[producttype] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[personal] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[local settings] HKLM\software\microsoft\windows Oueries value: nt\currentversion\winlogon[rsopdebuglevel] HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging] Oueries value: Oueries value: HKCU\software\microsoft\windows\currentversion\thememanager[compositing] Queries value: HKCU\control panel\desktop[lamebuttontext] Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[disableimprovedzonecheck] HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_protocol_lockdown[svchost.exe] HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_protocol_lockdown[*] HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-Queries value: ab78-1084642581fb1 HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-Queries value: 0000-0000000000000] Queries value: HKLM\system\currentcontrolset\control\computername\activecomputername[computername] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[fromcachetimeout] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[secureprotocols] HKLM\software\policies\microsoft\internet Queries value: explorer\main[security_hklm_only] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[certificaterevocation] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[disablekeepalive] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablepassport] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[idnenabled] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[cachemode] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[enablehttp1_1] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[proxyhttp1.1] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[enablenegotiate] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablebasicoverclearchannel] HKCU\software\microsoft\internet Oueries value: explorer\main\featurecontrol[feature_clientauthcertfilter] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol[feature clientauthcertfilter] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[clientauthbuiltinui] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[syncmode5] HKLM\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\cache[sessionstarttimedefaultdeltasecs] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache[signature] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\cache\content[peruseritem] $\label{lem:hklm} \verb+ HKLM \+ software \+ microsoft \+ windows \+ current version \+ internet$ Oueries value: settings\5.0\cache\content[peruseritem] Queries value: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}$ folders[cache] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\cache\content[cacheprefix] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[cachelimit] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[peruseritem] HKLM\software\microsoft\windows\currentversion\internet 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] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\cache\cookies[cachelimit]

settings\5.0\cache\cookies[peruseritem]

Oueries value:

```
Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
 Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}
 Oueries value:
folders[history]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
                           HKLM\software\microsoft\rpc[maxrpcsize]
 Oueries value:
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
settings\5.0\cache\extensible cache\domstore[cacherepair]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachepath]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cacheoptions]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cacherepair]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 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]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cachepath]
                           HKCU\software\microsoft\windows\currentversion\internet
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
 Queries 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:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\ietld[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\ietld[cachelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
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]
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ 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
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries 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
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Oueries value:
```

settings[disableworkerthreadhibernation]

```
Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[socketsendbufferlength]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketreceivebufferlength]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[keepalivetimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxhttpredirects]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsper1_0server]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsper1_0server]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperproxy]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries 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
 Oueries value:
settings[connectretries]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connectretries]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendtimeout]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[receivetimeout]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[receivetimeout]
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings[disablentlmpreauth]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[scavengecachelowerbound]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelimit]
 Oueries 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[svchost.exe]
 Queries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablecachingofsslpages]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[perusercookies]
                           \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
 Queries value:
settings[leashlegacycookies]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablent4rascheck]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[dialupuselansettings]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendextracrlf]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[bypassftptimecheck]
 Queries value:
                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[releasesocketduringauth]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[releasesocketduring401auth]
 Queries value:
                           \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
settings[releasesocketduring401auth]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
```

```
settings[wpadsearchalldomains]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[disablelegacypreauthasserver]
  Queries value:
                                      HKLM\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
  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[bypasshttpnocachecheck]
                                      \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
  Oueries value:
settings[bypasshttpnocachecheck]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
  Queries value:
                                      \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
settings[bypasssslnocachecheck]
  Oueries value:
                                      HKLM\software\microsoft\windows\currentversion\internet
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
  Queries value:
settings[dontusednsloadbalancing]
                                      HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dontusednsloadbalancing]
  Queries value:
                                      HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
                                      \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{$microsoft$} \windows \current version \sides \current} \end{tabular}
  Queries value:
settings[mimeexclusionlistforcache]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[headerexclusionlistforcache]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dnscacheenabled]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dnscacheentries]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnonpost]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnonzonecrossing]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertsending]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnonpostredirect]
  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[alwaysdrainonredirect]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 [serial\_access\_num] \ pr
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000006[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[packedcatalogitem]
  Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
  Oueries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 [serial\_access\_num]
```

Oueries value:

Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace_catalog5 \ (catalog_entries \ 00000000001[library path])$ Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 000000000001[displaystring]) \ displaystring \ (catalog_entries \ name space_catalog 5 \ (catalog_entries \ name space_ca$ Oueries value:

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

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace _catalog5 \ catalog_entries \ 000000000002 [library path]$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid] Oueries value:

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

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 00000000000002[supported name space]$ Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ no mespace_catalog \ set alog_entries \ (00000000000002 \ [enabled]) \ (enabled)$ Oueries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo] Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace _catalog5 \ catalog_entries \ 000000000003 [library path]$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000003[providerid] Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ (catalog_entries \ 000000000003 \ [address family]$ Oueries value:

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

Oueries value:

HKCU\software\microsoft\windows\currentversion\internet

Oueries value:

HKLM\svstem\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]

Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[enableautodial]

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

settings[urlencoding] Queries value:

settings[truncatefilename]

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

settings[badproxvexpirestime] HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_mime_handling[svchost.exe]

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

Queries value:

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

Queries value:

Oueries value:

HKLM\software\microsoft\tracing[enableconsoletracing] Oueries value: Oueries value:

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

HKLM\software\microsoft\tracing\rasapi32[filedirectory] Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell

folders[common appdata]

HKLM\software\microsoft\windows Oueries value:

nt\currentversion\profilelist[profilesdirectory]

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\profilelist[allusersprofile]

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\profilelist[defaultuserprofile]

HKLM\software\microsoft\windows\currentversion[programfilesdir] Oueries value: Queries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir]

Oueries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

1757981266-507921405-1957994488-1003[profileimagepath] Queries value: HKCU\software\microsoft\windows

nt\currentversion\winlogon[parseautoexec]

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

folders[appdata]

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

settings[migrateproxy]

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

settings[proxyenable]

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

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

settings\connections[savedlegacysettings]

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

settings\connections[defaultconnectionsettings]

HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll] Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow] Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh] Oueries value:

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

explorer\security[disablesecuritysettingscheck]

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

settings\zones\0[flags]

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

settings\zones\1[flags]

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

settings\zones\2[flags]

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

settings\zones\3[flags]

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

settings\zones\4[flags]

HKCU\software\microsoft\internet Queries value:

explorer\main\featurecontrol\feature localmachine lockdown[svchost.exe]

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

 $explorer \verb|\main\featurecontrol\feature_localmachine_lockdown[svchost.exe]|$

HKLM\software\microsoft\internet explorer\main\featurecontrol\feature localmachine lockdown[*1

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

settings[createuricachesize] HKLM\software\microsoft\windows\currentversion\internet Oueries value:

settings[createuricachesize]

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

settings[enablepunycode]

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

settings[enablepunycode]

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

settings\zonemap[autodetect]

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

settings\zones\3[1a10]

Queries value:

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

Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Oueries value:

 $HKLM \ system \ current control set \ services \ dns cache \ parameters [prioritize record data]$

HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]

Queries value:

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

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Oueries value:

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

Oueries value:

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

Oueries value:

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval] HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister] HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile] HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel] HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts] HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts] Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind] HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[enabledhcp] c7d49d7cecdc}[leaseobtainedtime] Queries value: $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4300-abe3-4300-a$ c7d49d7cecdc}[leaseterminatestime] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[dhcpserver]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain] Queries value:

```
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[queryadaptername]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[disableadapterdomainname]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registrationenabled]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registeradaptername]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registrationmaxaddresscount]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[maxnumberofaddressestoregister]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[domain]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpdomain]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[ipautoconfigurationenabled]
c7d49d7cecdc}[addresstype]
 Queries value:
c7d49d7cecdc}[nameserver]
c7d49d7cecdc}[dhcpnameserver]
                        HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
 Queries value:
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
                        HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
 Queries value:
cryptographic provider[type]
                       HKLM \verb|\software\microsoft\cryptography\defaults\provider\microsoft\ strong
 Queries value:
cryptographic provider[image path]
                       HKLM\software\microsoft\rpc\securityservice[10]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
                       HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
 Queries value:
 Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]
 Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]
                        HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrol\set\control\lsa\sspicache\msapsspc.dll[version]
                        HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]
 Queries value:
 Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]
                        HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]
 Queries value:
 Oueries value:
                        HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]
 Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities]
 Queries value:
                        HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid]
 Oueries value:
                        HKLM \ system \ current control \ sabspicache \ digest. dll[version]
 Queries value:
                        HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]
 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:
                        HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version]
 Queries value:
                        HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize]
 Queries value:
                        HKLM\software\microsoft\cryptography[machineguid]
 Oueries value:
                        HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
 Queries value:
                        HKLM\system\currentcontrolset\services\winsock\parameters[transports]
                        HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
 Queries value:
```

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \tcpip \parameters \winsock \mbox{[maxsockaddrlength]} \qed$ Queries value:

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
Queries value: HKCR\mime\database\content type\text/plain[extension]

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

 $\label{thm:local_transform} Value\ changes: \\ HKCU \ software \ microsoft \ windows \ current version \ explorer \ shell \\$

folders[cache]

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

folders[cookies]

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

folders[history]

 $\label{thm:local_problem} Value\ changes: \\ HKLM\ software\ microsoft\ windows\ current version\ (explorer\ shell). \\$

folders[common appdata]

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

folders[appdata]

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

settings[proxyenable]

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

settings\connections[savedlegacysettings]

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

settings\zonemap[proxybypass]

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

settings\zonemap[intranetname]

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

settings\zonemap[uncasintranet]

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

settings\zonemap[autodetect]