Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 101, Task ID: 403

Task ID: 403 Risk Level: 1

Date Processed: 2016-04-28 12:57:52 (UTC)

Processing Time: 61.39 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\00aca0729582792a46b971951043ff06.exe"

Sample ID: 101
Type: basic
Owner: admin

Label: 00aca0729582792a46b971951043ff06

Date Added: 2016-04-28 12:45:00 (UTC)

File Type: PE32:win32:gui File Size: 203723 bytes

MD5: 00aca0729582792a46b971951043ff06

SHA256: 0afff2c277d7116b78d29818c8a9422daea4846a70a311c1696f262597209006

Description: None

Pattern Matching Results

HTTP connection - response code 404 (file not found) [HTTP, GET, POST, web, network, response code]

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

Creates process: C:\WINDOWS\Temp\00aca0729582792a46b971951043ff06.exe

["c:\windows\temp\00aca0729582792a46b971951043ff06.exe"]

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

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-

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

File System Events

Creates: C:\WINDOWS\Temp\HandWalletUpdate.original

Opens: C:\WINDOWS\Prefetch\00ACA0729582792A46B971951043F-2EDA1F17.pf

Opens: C:\Documents and Settings\Admin

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

Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83

Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll

Opens: C:\WINDOWS\Temp\00aca0729582792a46b971951043ff06.exe

Opens: C:\WINDOWS\system32\imm32.dll
Opens: C:\WINDOWS\system32\shell32.dll

Opens: C:\WINDOWS\system32\shell32.dll.124.Manifest
Opens: C:\WINDOWS\system32\shell32.dll.124.Config

Opens: C:\WINDOWS\WindowsShell.Manifest
Opens: C:\WINDOWS\WindowsShell.Config

Opens: C:\WINDOWS\Temp

Opens: C:\WINDOWS\system32\MSCTF.dl1
Opens: C:\WINDOWS\system32\MSCTFIME.IME

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

Opens: C:\windows\temp\HandWalletUpdate.original

Opens: C:http:\www.handwallet.com\update\

 Opens:
 C:\WINDOWS\system32\urlmon.dll.123.Manifest

 Opens:
 C:\WINDOWS\system32\urlmon.dll.123.Config

 Opens:
 C:\WINDOWS\system32\WinINet.dll.123.Manifest

 Opens:
 C:\WINDOWS\system32\WinINet.dll.123.Config

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

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

Files\Content.IE5

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

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

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

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 C:\WINDOWS\system32\rasman.dll Opens: Opens: C:\WINDOWS\system32\netapi32.dll Opens: C:\WINDOWS\system32\tapi32.dll Opens: C:\WINDOWS\system32\rtutils.dll C:\WINDOWS\system32\winmm.dll Opens:

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

Opens: C:\AUT0EXEC.BAT

Opens: C:\

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

Data\Microsoft\Network\Connections\Pbk

Opens: C:\WINDOWS\system32\ras

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

Data\Microsoft\Network\Connections\Pbk\

Opens: C:\WINDOWS\system32\sensapi.dll Opens: C:\WINDOWS\system32\msv1_0.dll Opens: C:\WINDOWS\system32\iphlpapi.dll Opens: C:\WINDOWS\system32\mswsock.dll Opens: C:\WINDOWS\system32\rasadhlp.dll Opens: C:\WINDOWS\system32\dnsapi.dll Opens: C:\WINDOWS\system32\drivers\etc\hosts Opens: C:\WINDOWS\system32\rsaenh.dll C:\WINDOWS\system32\crypt32.dll Opens: Opens: C:\WINDOWS\system32\hnetcfg.dll Opens: C:\WINDOWS\system32\wshtcpip.dll

Opens: C:\WINDOWS\Temp\HandWalletUpdate.original
Opens: C:\windows\temp\HandWalletUpdate.info
Writes to: C:\WINDOWS\Temp\HandWalletUpdate.original

Reads from: C:\WINDOWS\Temp\00aca0729582792a46b971951043ff06.exe

Reads from: C:\AUT0EXEC.BAT

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

Reads from: C:\WINDOWS\Temp\HandWalletUpdate.original

Network Events

DNS query: www.handwallet.com

DNS response: handwallet.com ⇒ 198.71.157.117

Connects to: 198.71.157.117:80

Sends data to: 8.8.8.8:53

Sends data to: handwallet.com:80 (198.71.157.117)

Receives data from: 0.0.0.0:0

Receives data from: handwallet.com:80 (198.71.157.117)

Windows Registry Events

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

folders

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

Creates key: HKLM\software\microsoft\tracing

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

folders

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

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

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

 $\verb|settings\connections||$

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]

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

options\00aca0729582792a46b971951043ff06.exe

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

Opens key:

HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\system\currentcontrolset\control\safeboot\option

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

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

options\gdi32.dll

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

options\user32.dll

Opens key: HKLM\system\currentcontrol\session manager

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

options\imm32.dll

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

options\ntdll.dll

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

options\kernel32.dll

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

options\secur32.dll

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

options\rpcrt4.dll

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

options\advapi32.dll

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

options\msvcrt.dll

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

options\ole32.dll

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

options\oleaut32.dll

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

options\shlwapi.dll

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

options\shell32.dll

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

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\

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

Opens key: HKLM\software\microsoft\ole

Opens key: HKCR\interface

Opens key: HKCR\interface\{00020400-0000-c000-000000000046}

Opens key: HKLM\software\microsoft\oleaut

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

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

Opens key: HKLM\system\setup

Opens key: HKCU\

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

Opens key: HKCU\control panel\desktop

 $\label{lem:constant} \mbox{ Opens key:} & \mbox{ HKCU\software\microsoft\windows\currentversion\explorer\advanced } \\ \mbox{ HKLM\software\microsoft\windows nt\currentversion\languagepack }$

Opens key: HKCU\software\borland\locales
Opens key: HKLM\software\borland\locales
Opens key: HKCU\software\borland\delphi\locales

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

options\msctf.dll

Opens key:

 $HKLM \setminus software \setminus microsoft \setminus ctf \setminus compatibility \setminus 00aca0729582792a46b971951043ff06.exe \\$

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

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

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

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

options\version.dll

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

options\msctfime.ime

Opens key: HKCU\software\microsoft\ctf

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

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

options\uxtheme.dll

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

Opens key: HKCU\software\pantaray\qsetup\autoupdate

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\normaliz.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\iertutil.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: options\urlmon.dll Opens key: HKCU\software\classes\ HKCU\software\classes\protocols\name-space handler\ Opens key: Opens key: HKCR\protocols\name-space handler Opens key: HKCU\software\classes\protocols\name-space handler HKCU\software\policies\microsoft\windows\currentversion\internet Opens key: settings Opens key: HKLM\software\microsoft\windows\currentversion\internet settings Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} on the constraint of the$ Opens key: settings\ Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\ HKCU\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zonemap\domains\ Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\ 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: HKCU\software\microsoft\windows\currentversion\internet settings Opens key: HKLM\software\policies HKCU\software\policies Opens key: Opens key: HKCU\software Opens kev: HKLM\software Opens key: HKLM\software\policies\microsoft\internet explorer Opens key: HKLM\software\policies\microsoft\internet explorer\main Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content HKLM\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\content HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\cookies Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\cache\history HKLM\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\cache\history HKLM\software\microsoft\rpc\pagedbuffers Opens key: Opens key: HKLM\software\microsoft\rpc HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: options\00aca0729582792a46b971951043ff06.exe\rpcthreadpoolthrottle Opens kev: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKLM\system\currentcontrolset\control\computername Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername Opens key: $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ settings\5.0\cache\extensible cache Opens key: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}$ settings\5.0\cache\extensible cache\domstore HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\extensible cache\feedplat Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\iecompat Opens key: HKCU\software\microsoft\windows\currentversion\internet

```
settings\5.0\cache\extensible cache\ietld
                                   HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\extensible cache\mshist012014033120140407
                                   HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\extensible cache\mshist012014041220140413
  Opens key:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
  Opens key:
                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key:
                                   HKLM\software\microsoft\internet
\verb|explorer\main\featurecontrol\retry_header on ly post\_on connection reset|\\
  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
                                   HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
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\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:
                                  HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:
                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
  Opens key:
                                  HKLM\software\microsoft\internet
\verb|explorer| \verb|main| featurecontrol| feature\_use\_spn\_for\_ntlm\_auth\_disabled| \\
                                   HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_allow_long_international_filenames
  Opens key:
                                  HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
                                  HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
                                  HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
  Opens key:
                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
  Opens key:
                                  HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_disable\_unicode\_handle\_closing\_callback| \\
  Opens key:
                                  HKCU\software\microsoft\internet
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
                                  HKCU\software\microsoft\internet
  Opens key:
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:
                                   \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the current version \end{tabul
options\ws2help.dll
  Opens kev:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
                                   HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens kev:
  Opens key:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus protocol\_catalog 9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens kev:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000004
  Opens key:
```

Opens key:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
  Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ parameters \ protocol\_catalog\_entries \ protocol\_catalog \ parameters \ parameters
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000011
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  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:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\internet settings\wpad
                                       HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
                                       HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens 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:
                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winmm.dll
                                       HKLM\software\microsoft\windows nt\currentversion\drivers32
  Opens kev:
  Opens key:
\label{lem:hklm} \verb+Kklm \software \verb+ microsoft \verb+ windows nt \verb+ current version \verb+ image file execution \\
  Opens key:
options\tapi32.dll
                                       HKLM\software\microsoft\windows\currentversion\telephony
  Opens key:
  Opens kev:
                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasapi32.dll
  Opens kev:
                                       HKLM\software\microsoft\tracing\rasapi32
  Opens key:
                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\userenv.dll
  Opens key:
                                       HKLM\system\currentcontrolset\control\productoptions
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Opens key:
                                       HKLM\software\policies\microsoft\windows\system
  Opens key:
                                       HKLM\software\microsoft\windows nt\currentversion\profilelist
  Opens key:
                                       HKLM\system\currentcontrolset\control\session manager\environment
  Opens key:
                                       {\it HKLM \ } software \ \\ microsoft \ \\ windows \ \\ current version
                                       HKU\
  Opens kev:
                                       Opens key:
1757981266-507921405-1957994488-1003
                                       HKCU\environment
  Opens key:
                                       HKCU\volatile environment
  Opens key:
  Opens key:
                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
```

options\sensapi.dll

 ${\it HKLM} \verb|\software\microsoft\pc\securityservice|$ Opens key:

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

Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll Opens key: $HKLM \ system \ current control \ lsa \ sspicache \ msnsspc. dll$ Opens key: ${\tt HKLM \ } system \verb|\ current control \ } security providers \verb|\ sasl profiles \ |$ Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\iphlpapi.dll

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

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

options\msv1_0.dll

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_http_username_password_disable

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_http_username_password_disable

Opens key: HKCU\software\microsoft\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 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_include_port_in_spn_kb908209 Opens key: HKCU\software\microsoft\internet 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\mswsock.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasadhlp.dll $\label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\$ Opens key: settings\zonemap\ Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature zones check zonemap policy kb941001 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\ranges\ HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\zonemap\protocoldefaults\ Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\domains\ HKLM\software\microsoft\windows\currentversion\internet Opens key: settings\zonemap\domains\ HKLM\software\microsoft\windows\currentversion\internet Opens key: settings\zonemap\domains\msn.com Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\zonemap\domains\msn.com\related Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination HKCU\software\microsoft\internet explorer\ietld Opens key: HKLM\software\policies\microsoft\internet explorer\security Opens kev: 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 kev: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\ HKCU\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zones\ Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ settings\zones\0 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\0 HKLM\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\zones\1 Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}$ settings\zones\1 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\2 HKCU\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\zones\2 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\3 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\3 HKLM\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\zones\4 HKCU\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\zones\4 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown Opens kev: HKLM\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\ Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\ HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\lockdown_zones\ Opens key: HKCU\software\microsoft\windows\currentversion\internet

HKLM\software\policies\microsoft\windows\currentversion\internet

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

settings\lockdown_zones\0

settings\lockdown_zones\0

settings\lockdown_zones\0

Opens key:

Opens key:

```
Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
  Opens key:
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\1
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
  Opens key:
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\2
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
  Opens key:
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\3
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
  Opens key:
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\4
                                     HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
                                     HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\dnsapi.dll
  Opens key:
                                     HKLM\system\currentcontrolset\services\dnscache\parameters
                                     HKLM\software\policies\microsoft\windows nt\dnsclient
  Opens key:
  Opens key:
                                     HKLM\system\currentcontrolset\services\tcpip\parameters
  Opens key:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-a
c7d49d7cecdc}
                                     HKLM\software\policies\microsoft\system\dnsclient
  Opens kev:
  Opens key:
                                     HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\rsaenh.dll
  Opens key:
                                     HKLM\software\policies\microsoft\cryptography
                                     HKLM\software\microsoft\cryptography
  Opens kev:
  Opens key:
                                     HKLM\software\microsoft\cryptography\offload
  Opens key:
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\hnetcfg.dll
  Opens key:
                                     \label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ 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
                                     HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Oueries value:
  Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:
                                     HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
                                     HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\gre_initialize[disablemetafiles]
  Oueries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\compatibility32[00aca0729582792a46b971951043ff06]
  Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[00aca0729582792a46b971951043ff06]
  Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
  Oueries value:
                                     HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
  Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
  Queries value:
                                     HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
                                     HKLM\software\microsoft\ole[rwlockresourcetimeout]
  Oueries value:
  Queries value:
                                     HKCR\interface[interfacehelperdisableall]
  Oueries value:
                                     HKCR\interface[interfacehelperdisableallforole32]
  Queries value:
                                     HKCR\interface[interfacehelperdisabletypelib]
                                     HKCR\interface\{00020400-0000-0000-c000-
  Oueries value:
00000000046}[interfacehelperdisableall]
                                     HKCR\interface\{00020400-0000-0000-c000-
  Oueries value:
00000000046}[interfacehelperdisableallforole32]
  Queries value:
                                     HKLM\system\setup[systemsetupinprogress]
  Queries value:
                                     HKCU\control panel\desktop[multiuilanguageid]
                                     HKCU\control panel\desktop[smoothscroll]
  Oueries value:
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
  Oueries value:
                                     HKLM\software\microsoft\ctf\systemshared[cuas]
  Oueries value:
                                     HKCU\keyboard layout\toggle[language hotkey]
  Queries value:
                                     HKCU\keyboard layout\toggle[hotkey]
```

HKCU\keyboard layout\toggle[layout hotkey]

HKLM\software\microsoft\ctf[enableanchorcontext]

Oueries value:

Oueries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]

Oueries value: HKCU\software\microsoft\ctf[disable thread input manager]

Oueries value: HKCU\software\microsoft\windows\currentversion\thememanager[compositing]

Queries value: HKCU\control panel\desktop[lamebuttontext]

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

settings[disableimprovedzonecheck]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_protocol_lockdown[00aca0729582792a46b971951043ff06.exe]

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

Oueries value: HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-

ab78-1084642581fb]

Queries value: HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-

0000-0000000000001

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

settings[fromcachetimeout]

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

settings[secureprotocols]

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

explorer\main[security_hklm_only]

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

settings[certificaterevocation]

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

settings[disablekeepalive]

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

settings[disablepassport]

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

settings[idnenabled]

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

settings[cachemode]

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

settings[enablehttp1_1]

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

settings[proxyhttp1.1]

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

settings[enablenegotiate]

Oueries value:

HKCU\software\microsoft\windows\currentversion\internet settings[disablebasicoverclearchannel]

Queries value:

HKCU\software\microsoft\internet explorer\main\featurecontrol[feature clientauthcertfilter] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol[feature_clientauthcertfilter]

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

settings[clientauthbuiltinui]

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

settings[syncmode5]

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

settings\5.0\cache[sessionstarttimedefaultdeltasecs]

HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\cache[signature]

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

settings\5.0\cache\content[peruseritem] HKLM\software\microsoft\windows\currentversion\internet

Queries value: settings\5.0\cache\content[peruseritem]

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

folders[cache]

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

settings\5.0\cache\content[cacheprefix]

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

settings\5.0\cache\content[cachelimit]

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

settings\5.0\cache\cookies[peruseritem]

 $\label{lem:hklm} \verb+ HKLM \+ software \+ microsoft \+ windows \+ current version \+ internet$ Queries value:

settings\5.0\cache\cookies[peruseritem]

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

folders[cookies]

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

settings\5.0\cache\cookies[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\cookies[cachelimit]

Queries value:

HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\history[peruseritem]

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

settings\5.0\cache\history[peruseritem] HKCU\software\microsoft\windows\currentversion\explorer\user shell

Queries value:

folders[history]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\history[cacheprefix]

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

settings\5.0\cache\history[cachelimit]

Queries value: HKLM\software\microsoft\rpc[maxrpcsize]

Oueries value:

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

```
settings[maxhttpredirects]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsperserver]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
 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[maxconnectionsper1_0server]
 Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperproxy]
 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[serverinfotimeout]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connecttimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connectretries]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connectretries]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendtimeout]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendtimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[receivetimeout]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[receivetimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablentlmpreauth]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[scavengecachelowerbound]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[certcachenovalidate]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelifetime]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirvtimesecs]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
                           HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[00aca0729582792a46b971951043ff06.exe]
 Queries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature disable unicode handle closing callback[*1
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[perusercookies]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[leashlegacycookies]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablent4rascheck]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dialupuselansettings]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dialupuselansettings]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypassftptimecheck]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[releasesocketduringauth]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[releasesocketduring401auth]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablelegacypreauthasserver]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasshttpnocachecheck]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasssslnocachecheck]
```

```
Oueries value:
                         HKLM\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries 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
 Oueries value:
settings[dontusednsloadbalancing]
                         HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sharecredswithwinhttp]
                         \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
 Queries value:
settings[mimeexclusionlistforcache]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[headerexclusionlistforcache]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dnscacheenabled]
                         \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
 Queries value:
settings[dnscacheentries]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dnscachetimeout]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonpost]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnalwaysonpost]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonzonecrossing]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonbadcertsending]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[alwaysdrainonredirect]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonhttpstohttpredirect]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000008[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
 Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 0000000000010 \ [packed catalog item]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
 Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000001 \ [address family]
```

```
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000001[supported name space]]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ set alog\_entries \ (0000000000001[version]) \ details \ det
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000002[librarypath]
   Oueries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ catalog\_entries \ 0000000000002 \ [displaystring]
   Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
   Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
   Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog 5 \setminus catalog\_entries \setminus 00000000000002[storesserviceclass info]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ (catalog\_entries \ 0000000000003 \ [displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[addressfamily]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000003 \ [supported name space]
   Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap services \setminus catalog \le catalog \le catalog \le catalog = not in the control set \setminus services \setminus catalog \le catalo
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
                                             HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[enableautodial]
   Queries value:
                                             HKLM\software\microsoft\windows\currentversion\internet
settings[urlencoding]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[truncatefilename]
                                             HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[badproxyexpirestime]
   Queries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
   Oueries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
   Queries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
   Queries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
   Oueries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
   Oueries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
   Queries value:
   Queries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
   Oueries value:
                                             HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 8]
   Queries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
   Oueries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[midil
   Oueries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
   Oueries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
   Queries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
   Queries value:
                                             HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [midi4]
   Queries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
   Oueries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi61]
   Queries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
   Oueries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
   Oueries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi91
   Queries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
   Queries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
   Oueries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
   Queries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
   Oueries value:
                                             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
```

HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]

HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]

HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]

HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]

HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]

Oueries value:

Oueries value:

Queries value:

Oueries value:

```
Oueries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
 Queries value:
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
 Oueries value:
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32\mixer81
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
 Oueries value:
Oueries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32requestretrytimeout]
 Oueries value:
                         HKLM\software\microsoft\tracing[enableconsoletracing]
 Queries value:
                         HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
 Queries value:
                         HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
 Oueries value:
                         HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
 Queries value:
                         HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
 Queries value:
                         HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
                         HKLM\software\microsoft\tracing\rasapi32[filedirectory]
 Oueries value:
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common appdata]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\winlogon[userenvdebuglevel]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\winlogon[chkaccdebuglevel]
                         HKLM\system\currentcontrolset\control\productoptions[producttype]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Oueries value:
folders[personal]
                         HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Queries value:
folders[local settings]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\winlogon[rsopdebuglevel]
                         HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
 Oueries value:
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\profilelist[profilesdirectory]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\profilelist[allusersprofile]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\profilelist[defaultuserprofile]
                         HKLM\software\microsoft\windows\currentversion[programfilesdir]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion[commonfilesdir]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
 Queries value:
1757981266-507921405-1957994488-1003[profileimagepath]
                         HKCU\software\microsoft\windows
 Queries value:
nt\currentversion\winlogon[parseautoexec]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[migrateproxy]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[proxyenable]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[proxyoverride]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[autoconfigurl]
                         \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings\connections[savedlegacysettings]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\connections[defaultconnectionsettings]
                         HKLM\software\microsoft\rpc\securityservice[10]
 Oueries value:
 Queries value:
HKLM \setminus system \setminus current control \setminus security providers [security providers]
 Queries value:
                         HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
 Queries value:
                         HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
 Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]
 Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]
 Oueries value:
                         HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]
 Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[version]
                         HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]
                         HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]
 Oueries value:
```

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

Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities] $HKLM \setminus system \setminus current control \setminus lsa \setminus sspicache \setminus digest. \\ dll[rpcid]$ Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version] Queries value: Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize] HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment] Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid] Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version] Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize] HKLM\software\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_mime_handling[00aca0729582792a46b971951043ff06.exe] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling[*] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll] Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow] HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh] Oueries value: Queries value: HKLM\software\policies\microsoft\internet explorer\security[disablesecuritysettingscheck] $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}$ Queries value: settings\zones\0[flags] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\1[flags] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[flags] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\3[flags] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[flags] HKCU\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_localmachine_lockdown[00aca0729582792a46b971951043ff06.exe] HKCU\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_localmachine_lockdown[*] HKLM\software\microsoft\internet Queries value: HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_localmachine_lockdown[*] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[createuricachesize] HKLM\software\microsoft\windows\currentversion\internet Queries value: settings[createuricachesize] Queries value: $\label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\$ settings[enablepunycode] Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[enablepunycode] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zonemap[autodetect] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1a10] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname] HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata] 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] HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers] 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]

```
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]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
 Oueries 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]
 Queries value:
Queries value:
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]
 Oueries value:
                      HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
                      HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
 Queries value:
                      HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
 Oueries value:
 Oueries value:
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]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
 Oueries value:
                      HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
c7d49d7cecdc}[enabledhcp]
c7d49d7cecdc}[leaseobtainedtime]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[leaseterminatestime]
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpserver]
 Queries value:
                      HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
                      \label{lem:hklm} \verb+Kklm \system \current control set \services \tcpip \parameters [domain]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[queryadaptername]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[disableadapterdomainname]
 Queries value:
```

```
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]
 Oueries 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}[addresstvpe]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[nameserver]
 Queries value:
c7d49d7cecdc}[dhcpnameserver]
                      HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
 Queries value:
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
                       HKLM \verb|\software\m| icrosoft \verb|\cryptography\defaults\provider\m| icrosoft strong
 Queries value:
cryptographic provider[type]
                      HKLM \ software \ microsoft \ strong
 Queries value:
cryptographic provider[image path]
 Queries value:
                      HKLM\software\microsoft\cryptography[machineguid]
                      HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
 Oueries value:
 Queries value:
                       HKLM\system\currentcontrolset\services\winsock\parameters[transports]
 Queries value:
                      HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
                       HKLM\software\microsoft\crvptographv\rng[seed]
 Value changes:
 Value changes:
                       HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
 Value changes:
                       HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cookies]
                       HKCU\software\microsoft\windows\currentversion\explorer\shell
 Value changes:
folders[history]
 Value changes:
                       HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common appdata]
 Value changes:
                      HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[appdata]
 Value changes:
                       HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
                       \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Value changes:
```

HKCU\software\microsoft\windows\currentversion\internet

HKCU\software\microsoft\windows\currentversion\internet

HKCU\software\microsoft\windows\currentversion\internet

HKCU\software\microsoft\windows\currentversion\internet

settings\connections[savedlegacysettings]

settings\zonemap[proxybypass]

settings\zonemap[intranetname]

settings\zonemap[uncasintranet]

settings\zonemap[autodetect]

Value changes:

Value changes:

Value changes:

Value changes: