Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 54, Task ID: 215

Task ID: 215 Risk Level: 4

Date Processed: 2016-04-28 12:53:12 (UTC)

Processing Time: 7.95 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\607c7d18e490c5b56e91c74a29ae3e0a.exe"

Sample ID: 54
Type: basic
Owner: admin

Label: 607c7d18e490c5b56e91c74a29ae3e0a

Date Added: 2016-04-28 12:44:55 (UTC)
File Type: PF32:win32:gui

File Type: PE32:win32:gui File Size: 106104 bytes

MD5: 607c7d18e490c5b56e91c74a29ae3e0a

SHA256: 006257143f3aa20ebc8a51441005feee0cce6d81bca404356d3c1cb657345b9e

Description: None

Pattern Matching Results

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

2 PE: Nonstandard section

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

Packer: NSIS [Nullsoft Scriptable Install System]

Static Events

Anomaly: PE: Contains a virtual section

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

Process/Thread Events

Creates process: C:\WINDOWS\Temp\607c7d18e490c5b56e91c74a29ae3e0a.exe

["c:\windows\temp\607c7d18e490c5b56e91c74a29ae3e0a.exe"]

Loads service: RASMAN [C:\WINDOWS\system32\svchost.exe -k netsvcs]
Terminates process: C:\WINDOWS\Temp\607c7d18e490c5b56e91c74a29ae3e0a.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\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 event: \BaseNamedObjects\userenv: User Profile setup event

 $\label{lem:continuous} $$\operatorname{Semaphore}: $$\operatorname{S$

File System Events

Creates: C:\DOCUME~1\Admin\LOCALS~1\Temp\

Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nsi1.tmp
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nss2.tmp
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nsc3.tmp

Creates: C:\DOCUME~1
Creates: C:\DOCUME~1\Admin

Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nsc3.tmp\System.dll

Creates: C:\DOCUME~1\Admin\LOCALS~1\Temp\nsc3.tmp\System.dll

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

Settings\Temp\nsc3.tmp\zplugins.dll

Creates: C:\DOCUME~1\Admin\LOCALS~1\Temp\nsc3.tmp\zplugins.dll

Creates: C:\Documents and Settings\Admin\Local Settings\Temp\28C507DB-D7FB-4AEC-

9C80-02EC74BC9D8C

```
C:\Documents and Settings\Admin\Local Settings\Temp\nsc3.tmp\result.txt
  Creates:
                                      C:\WINDOWS\Prefetch\607C7D18E490C5B56E91C74A29AE3-2BD7784E.pf
  Opens:
  Opens:
                                      C:\Documents and Settings\Admin
                                      C:\WINDOWS\system32\imm32.dll
  Opens:
  Opens:
                                      C:\WINDOWS\system32\shell32.dll
  Opens:
                                      C:\WINDOWS\system32\SHELL32.dll.124.Manifest
                                      C:\WINDOWS\system32\SHELL32.dll.124.Config
  Opens:
                                      C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
  Opens:
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
                                      C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
  Opens:
                                      C:\WINDOWS\WindowsShell.Manifest
  Opens:
                                      C:\WINDOWS\WindowsShell.Config
                                      C:\WINDOWS\Temp\607c7d18e490c5b56e91c74a29ae3e0a.exe
  Opens:
  Opens:
                                      C:\windows\temp\607c7d18e490c5b56e91c74a29ae3e0a.exe.124.Manifest
                                      C:\WINDOWS\system32\comctl32.dll
  Opens:
  Opens:
                                      C:\WINDOWS\system32\COMCTL32.dll.124.Manifest
  Opens:
                                      C:\WINDOWS\system32\COMCTL32.dll.124.Config
  Opens:
                                      C:\WINDOWS\system32\rpcss.dll
  Opens:
                                      C:\WINDOWS\system32\MSCTF.dll
  Opens:
                                      C:\WINDOWS\system32\shfolder.dll
  Opens:
                                      C:\WINDOWS\system32\setupapi.dll
  Opens:
                                      C:\
  Opens:
                                      C:\Documents and Settings
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Temp\nsi1.tmp
                                      C:\WINDOWS\Temp\c9db03d7-ecdc-4d4b-8fe6-b97d40162578
  Opens:
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Temp
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Temp\nsc3.tmp
                                      C:\Documents and Settings\Admin\Local Settings\Temp\nsc3.tmp\System.dll
  Opens:
  Opens:
                                      C:\Documents and Settings\Admin\Local
Settings\Temp\nsc3.tmp\zplugins.dll
                                      C:\DOCUME~1\Admin\LOCALS~1\Temp\nsc3.tmp\zplugins.dll.2.Manifest
  Opens:
  Opens:
                                      \label{locals-1} C: \verb|\DOCUME-1| Admin| LOCALS-1| Temp| nsc3.tmp| zplugins.dll.2.Config| and the configuration of the configuration o
  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
                                      C: \verb|\DOCUME-1| Admin \verb|\LOCALS-1| Temp \verb|\28C507DB-D7FB-4AEC-9C80-02EC74BC9D8C| \\
  Opens:
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\History
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\History\History.IE5
                                      C:\Documents and Settings\Admin\Local Settings\Temporary Internet
  Opens:
Files\Content.IE5\index.dat
  Opens:
                                      C:\Documents and Settings\Admin\Cookies
                                      C:\Documents and Settings\Admin\Cookies\index.dat
  Opens:
  Opens:
                                      C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\index.dat
                                      C:\WINDOWS\system32\ws2_32.dll
  Opens:
  Opens:
                                      C:\WINDOWS\system32\ws2help.dll
  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
  Opens:
                                      C:\WINDOWS\system32\winmm.dll
  Opens:
                                      C:\WINDOWS\system32\TAPI32.dll.124.Manifest
                                      C:\WINDOWS\system32\TAPI32.dll.124.Config
  Opens:
  Opens:
                                      C:\AUTOEXEC.BAT
  Opens:
                                      C:\Documents and Settings\All Users\Application
Data\Microsoft\Network\Connections\Pbk
                                      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\mswsock.dll
                                      C:\WINDOWS\system32\rasadhlp.dll
  Opens:
  Opens:
                                      C:\WINDOWS\system32\dnsapi.dll
  Opens:
                                      C:\WINDOWS\system32\iphlpapi.dll
                                      C:\WINDOWS\system32\drivers\etc\hosts
  Opens:
  Opens:
                                      C:\WINDOWS\system32\rsaenh.dll
  Opens:
                                      C:\WINDOWS\system32\msv1 0.dll
  Opens:
                                      C:\WINDOWS\system32\crypt32.dll
  Opens:
                                      C:\WINDOWS\system32\hnetcfg.dll
                                      C:\WINDOWS\system32\wshtcpip.dll
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Temp\28C507DB-D7FB-4AEC-
  Opens:
9C80-02EC74BC9D8C
                                      C:\Documents and Settings\Admin\Local Settings
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Temp\nsc3.tmp\result.txt
  Opens:
  Writes to:
                                      C:\Documents and Settings\Admin\Local Settings\Temp\nss2.tmp
                                      C:\Documents and Settings\Admin\Local Settings\Temp\nsc3.tmp\System.dll
  Writes to:
  Writes to:
                                      C:\Documents and Settings\Admin\Local
```

Settings\Temp\nsc3.tmp\zplugins.dll

Reads from: C:\WINDOWS\Temp\607c7d18e490c5b56e91c74a29ae3e0a.exe

Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\nss2.tmp

Reads from: C:\AUT0EXEC.BAT

Reads from: C:\WINDOWS\system32\drivers\etc\hosts

Reads from: C:\WINDOWS\system32\rsaenh.dll

Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsi1.tmp
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsc3.tmp

Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsc3.tmp\result.txt
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsc3.tmp\System.dll

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

Settings\Temp\nsc3.tmp\zplugins.dll

Network Events

DNS query: dl.distromatic.com
DNS query: utrack.n.distromatic.com

DNS response: $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.39$ DNS response: $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.176$ $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.203$ DNS response: DNS response: $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.19$ DNS response: $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.83$ DNS response: $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.221$ $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.106$ DNS response: DNS response: $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.98$ DNS response: utrack.n.distromatic.com ⇒ 52.87.82.229 DNS response: utrack.n.distromatic.com ⇒ 52.73.93.66

Connects to: 54.230.144.39:80
Connects to: 52.87.82.229:80
Sends data to: 8.8.8.8:53

Sends data to: d2624xgal0u1e4.cloudfront.net:80 (54.230.144.39)
Sends data to: utrack.n.distromatic.com:80 (52.87.82.229)

Receives data from: 0.0.0.0:0

Receives data from: d2624xgal0u1e4.cloudfront.net:80 (54.230.144.39)

Receives data from: utrack.n.distromatic.com:80 (52.87.82.229)

Windows Registry Events

Creates key:

806d6172696f}\ Creates key: Creates key:

HKCU\software\microsoft\windows\currentversion\internet settings
HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders

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

Creates kev: HKLM\software\microsoft\tracing

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

folders

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

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

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

settings\connections

 $\label{lem:creates} \begin{tabular}{lll} Creates key: & HKCU\software\microsoft\windows nt\currentversion\network\location \\ \end{tabular}$

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\607c7d18e490c5b56e91c74a29ae3e0a.exe

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

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

options\gdi32.dll

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

options\user32.dll

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

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

Opens key: options\imm32.dll

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

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

options\ntdll.dll

options\ntdil.dil
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\shlwapi.dll

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

options\comctl32.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\version.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\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\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

Opens key:

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

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack

Opens key: HKLM\software\microsoft\ole

Opens key: HKCR\interface

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

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

options\msctf.dll

Opens key:

HKLM\software\microsoft\ctf\compatibility\607c7d18e490c5b56e91c74a29ae3e0a.exe

Opens key: $\label{lem:hklmsoftware} \verb+MKLM\software\microsoft\ctf\systemshared\cite{lem:hklmsoftware} + \label{lem:hklmsoftware} \end{substitute}$

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

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

options\shfolder.dll

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

Opens key:

Opens key:

a2d8-08002b30309d}

Opens key: HKCU\software\classes\

Opens key: $\label{local-continuous} \mbox{HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-4cd}} \mbox{ HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-4cd}} \mbox{ HKCU\software\classes\clsid\$

08002b30309d}\inprocserver32

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

options\setupapi.dll

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

Opens key: HKLM\system\wpa\pnp

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

Opens key: HKLM\software\microsoft\windows\currentversion\setup\apploglevels
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key: HKLM\software\policies\microsoft\system\dnsclient

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\607c7d18e490c5b56e91c74a29ae3e0a.exe\rpcthreadpoolthrottle
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\system\currentcontrolset\control\computername

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\mountpoints2| cpc \volume | lem to be a constraint of the constrain$

Opens key: <CU\softwa Opens key:

11e3-9fc7-806d6172696f}\

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

Opens key: HKCR\drive\shellex\folderextensions

 $Opens~key: \\ HKCU \setminus software \\ \\ classes \\ \\ drive \setminus shellex \\ \\ folder extensions \\ \\ \{fbeb8a05-beee-drive\} \\ \\ folder extensions \\ \\ folder extensions$

4442-804e-409d6c4515e9}

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

409d6c4515e9}

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

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

Opens key: HKCR\directory\curver Opens key: HKCR\directorv\ HKCU\software\microsoft\windows\currentversion\explorer Opens key: HKCU\software\microsoft\windows\currentversion\explorer\ Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\policies\system Opens key: HKCU\software\classes\directory\shellex\iconhandler Opens key: HKCR\directory\shellex\iconhandler HKCU\software\classes\directory\clsid Opens key: Opens key: HKCR\directory\clsid HKCU\software\classes\folder Opens key: HKCR\folder Opens key: Opens key: HKCU\software\classes\folder\clsid Opens key: HKCR\folder\clsid HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\system.dll 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\oleaut32.dll HKLM\software\microsoft\oleaut Opens key: Opens key: HKLM\software\microsoft\oleaut\userera 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\protocols\name-space handler\ Opens key: Opens key: HKCR\protocols\name-space handler Opens key: HKCU\software\classes\protocols\name-space handler Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings Opens key: HKLM\software\microsoft\windows\currentversion\internet settings HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_protocol_lockdown HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\ HKLM\software\policies\microsoft\internet explorer\main\featurecontrol Opens key: Opens key: $\label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\internet\ explorer\mbox{\tt main\featurecontrol}} \\$ Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol HKCU\software\microsoft\internet explorer\main\featurecontrol Opens kev: Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ settings\zonemap\domains\ Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\ HKLM\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\zonemap\ranges\ $\label{lem:hkcu} \verb+KCU\+software\+policies\+microsoft\+windows\+currentversion\+internet$ Opens key: settings\zonemap\ranges\ Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wininet.dll Opens key: HKLM\system\currentcontrolset\control\wmi\security Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\zplugins.dll $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet}} \ \ \mbox{\tt settings} \ \ \mbox{\tt microsoft\windows\currentversion\color=lem:} \ \mb$ Opens key: Opens key: HKLM\software\policies Opens key: HKCU\software\policies HKCU\software Opens key: Opens key: HKLM\software Opens kev: HKLM\software\policies\microsoft\internet explorer Opens key: HKLM\software\policies\microsoft\internet explorer\main Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache

Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache\content
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies

```
HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\history
                          HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus internet
 Opens key:
settings\5.0\cache\history
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0\cache\extensible cache
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0\cache\extensible cache\iecompat
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\extensible cache\mshist012014041220140413
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\extensible cache\privacie:
                          HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
                          HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
                          HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_bufferbreaking_818408
                          HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
                         HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache
                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} internet \end{tabular}
 Opens key:
settings\5.0\cache
                          HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                          HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                          HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                          HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
                          HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature allow long international filenames
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature disable unicode handle closing callback
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                          HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                         HKLM\software\microsoft\internet
 Opens key:
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
                         HKLM\software\microsoft\internet
 Opens key:
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 kev:
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens kev:
```

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_http_username_password_disable

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

Opens key: HKLM\software\microsoft\internet
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

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

options\rtutils.dll
Opens kev: HKLN

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

options\winmm.dll

Opens key: ${\tt HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32}$

Opens key:

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

options\tapi32.dll

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

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

options\rasapi32.dll

Opens key: HKLM\software\microsoft\tracing\rasapi32

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

 ${\tt options \setminus userenv.dll}$

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\currentcontrol\session manager\environment

Opens key: HKU\

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

1757981266-507921405-1957994488-1003 Opens key: HKCU\environment

Opens 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

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

options\rasadhlp.dll

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

options\dnsapi.dll

Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient

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

options\iphlpapi.dll

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

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

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

Opens key:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-

c7d49d7cecdc}

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

 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\software\microsoft\cryptography\defaults\provider\microsoft strong

cryptographic provider

Opens key: HKLM\system\currentcontrolset\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: HKLM\software\policies\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography

Opens key: ${\tt HKLM \ } {\tt Software \ } {\tt Microsoft \ } {\tt cryptography \ } {\tt offload}$

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

options\hnetcfg.dll
 Opens key:

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

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

Queries value:

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

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

nt\currentversion\compatibility32[607c7d18e490c5b56e91c74a29ae3e0a]

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

compatibility[607c7d18e490c5b56e91c74a29ae3e0a]

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

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

Oueries value:

 $HKCU \ software \ microsoft \ windows \ current version \ (explorer \ advanced [enable balloon tips]) \ described by the software \ (explorer) \ described by$

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

manager[criticalsectiontimeout]

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

Queries value: HKCR\interface[interfacehelperdisableall]

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

00000000046}[interfacehelperdisableall]

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

00000000046}[interfacehelperdisableallforole32]

 Queries value:
 HKLM\software\microsoft\ctf\systemshared[cuas]

 Queries value:
 HKCU\keyboard layout\toggle[language hotkey]

 Queries value:
 HKCU\keyboard layout\toggle[hotkey]

 Queries value:
 HKCU\keyboard layout\toggle[layout hotkey]

 Queries value:
 HKLM\software\microsoft\ctf[enableanchorcontext]

Queries value:

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

Queries value:

Queries value:

 $\label{thm:local_hammon} \begin{tabular}{l} HKCU \software \verb|\microsoft| windows \current version \policies \explorer[nointerneticon] \end{tabular}$

Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders] $\label{local-condition} HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\ \ inprocserver32[]$ Oueries value: HKLM\system\wpa\pnp[seed] Oueries value: Oueries value: HKLM\system\setup[osloaderpath] Queries value: HKLM\system\setup[systempartition] HKLM\software\microsoft\windows\currentversion\setup[sourcepath] Oueries value: Queries value: HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath] Oueries value: HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath] Queries value: HKLM\software\microsoft\windows\currentversion\setup[drivercachepath] HKI M\software\microsoft\windows\currentversion[devicepath] Oueries value: Queries value: HKLM\software\microsoft\windows\currentversion\setup[loglevel] Oueries value: HKLM\software\microsoft\windows\currentversion\setup[logpath] Oueries value: HKLM\system\currentcontrolset\control\computername\activecomputername[computername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain] Queries value: HKLM\software\microsoft\rpc[maxrpcsize] Queries value: 11e3-9fc7-806d6172696f}[data] Queries value: 11e3-9fc7-806d6172696f}[generation] HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-Oueries value: 409d6c4515e9}[drivemask] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[forceactivedesktopon] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop] Queries value: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\policies\explorer[nowebview]}}$ HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess] Queries value: $HKCU \ software \ microsoft \ windows \ current version \ policies \ explorer [nonet crawling]$ HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden] HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor1 HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons] Queries value: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \mbox{\mathbb{N} indows \current version \explorer \advanced [mapnetdrvbtn]} \end{tabular}$ HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview] HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter] Oueries value: $\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{tabular} is a constant \cite{tabular} and \cite{tabular} is a constant \cite{tabular} and \cite{tabular} is a constant \cite{tabular} is a constant \cite{tabular} and \$ Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling] HKCR\directory[docobject] Oueries value: Oueries value: HKCR\directory[browseinplace] Oueries value: HKCR\directory[isshortcut] Queries value: HKCR\directory[alwaysshowext] Oueries value: HKCR\directory[nevershowext] Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[disableimprovedzonecheck]

Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[607c7d18e490c5b56e91c74a29ae3e0a.exe]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
Queries value: HKLM\system\currentcontrol\set\control\wmi\security[df8480a1-7492-4f45-

```
ab78-1084642581fb]
 Oueries value:
                           HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
0000-0000000000000]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
                          HKLM\software\policies\microsoft\internet
 Oueries value:
explorer\main[security_hklm_only]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
 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[disablekeepalive]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablepassport]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries 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]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablebasicoverclearchannel]
                          HKCU\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
                          HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[clientauthbuiltinui]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[signature]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\content[peruseritem]
                          \label{lem:hklm} \verb+Kklm\+ software\+ icrosoft\+ windows\+ current version\+ internet
 Queries value:
settings\5.0\cache\content[peruseritem]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cacheprefix]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cachelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
                          HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\cookies[peruseritem]
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Queries value:
folders[cookies]
 Queries 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]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\history[peruseritem]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Oueries value:
folders[history]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\history[cacheprefix]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cacherepair]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachepath]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheprefix]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheoptions]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\feedplat[cachepath]
```

```
Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cacherepair]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
                            \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ 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]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\ietld[cacheprefix]
                            \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ 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]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablereadrange]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketsendbufferlength]
 Queries value:
                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[socketreceivebufferlength]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[keepalivetimeout]
 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[maxhttpredirects]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
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]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries 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
 Oueries value:
settings[connecttimeout]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[connectretries]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendtimeout]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
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]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[ftpdefaultexpirytimesecs]
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[607c7d18e490c5b56e91c74a29ae3e0a.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]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[leashlegacycookies]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[disablent4rascheck]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
                          HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dialupuselansettings]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[bypassftptimecheck]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[releasesocketduringauth]
 Queries value:
                          \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[releasesocketduring401auth]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[wpadsearchalldomains]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablelegacypreauthasserver]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasshttpnocachecheck]
 Oueries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
                          HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasssslnocachecheck]
 Oueries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
                          HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[nocheckautodialoverride]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                          HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sharecredswithwinhttp]
```

```
HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
  Oueries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[dnscacheenabled]
  Queries value:
                                   \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
settings[dnscacheentries]
  Queries value:
                                   \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
settings[dnscachetimeout]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonpost]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnalwaysonpost]
                                   \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
  Queries value:
settings[warnonzonecrossing]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonbadcertsending]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnonbadcertrecving]
                                   \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
  Queries value:
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]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9[num catalog entries]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
  Oueries value:
Queries value:
Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries \ 0000000000004 \ [packed catalog item]
  Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000006[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000009[packedcatalogitem]
  Queries 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\currentcontrolset\services\winsock2\parameters\namespace catalog5[serial access num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
  Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace \_catalog5 \ catalog\_entries \ 000000000001 [library path]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
  Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 00000000001 \ [address family]
  Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000001[supported name space]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_\catalog_entries\00000000001[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000002[librarypath]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
  Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ name space\_catalog \ name space\_cat
```

Oueries value:

Queries value:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace\_catalog 5 \setminus catalog\_entries \setminus 0000000000002[supported names pace]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus names pace\_catalog \\ \setminus catalog\_entries \setminus 00000000000002[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]
  Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ (catalog\_entries \ 00000000003 \ [library path]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
  Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog5 \ (catalog\_entries \ 0000000000003 \ [address family]
  Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog 5 \setminus catalog\_entries \setminus 0000000000003 [version]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[globaluseroffline]
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings[enableautodial]
                           HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[urlencoding]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[truncatefilename]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[badproxyexpirestime]
                           HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_mime_handling[607c7d18e490c5b56e91c74a29ae3e0a.exe]
                           HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature mime handling[*]
  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 \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 3]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midill
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi41]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
  Queries value:
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
  Oueries value:
                           HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [midi8]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
  Queries value:
                           \label{lem:hklm} \mbox{ HKLM\software\mbox{\sc microsoft\windows nt\currentversion\drivers} 32[aux4] \\
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
  Oueries 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[mixer3]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
```

HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]

Queries value:

Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9] Oueries value:

HKLM\software\microsoft\windows\currentversion\telephony[tapi32maxnumrequestretries] Oueries value:

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

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

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

folders[common appdata]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\winlogon[userenvdebuglevel]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\winlogon[chkaccdebuglevel]

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

folders[personal]

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

folders[local settings]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\winlogon[rsopdebuglevel]

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

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

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

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

nt\currentversion\winlogon[parseautoexec]

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

folders[appdata]

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

settings[migrateproxv]

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

settings[proxyenable]

HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[proxyserver]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyoverride]

Queries value:

settings[autoconfigurl]

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

settings\connections[savedlegacysettings]

Queries value:

settings\connections[defaultconnectionsettings] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]

HKCU\software\microsoft\windows\currentversion\internet

Oueries value:

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

Oueries value:

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

Queries value: Queries value:

HKLM\svstem\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]

Queries value:

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

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [prioritize record data]$ Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] Queries value:

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

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[guervipmatching] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [registration enabled]$ Queries 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] Queries 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] Queries 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[registrationtt1] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Queries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount] Queries value: $HKLM \verb| system| current control set \verb| services| tcpip| parameters[maxnumber of addresses to register]$ Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [update top level domain zones]$ HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts] HKLM\system\currentcontrolset\services\tcpip\linkage[bind] Queries value: Oueries value: c7d49d7cecdc}[enabledhcp] Queries value: c7d49d7cecdc}[leaseobtainedtime] Oueries value: c7d49d7cecdc}[leaseterminatestime] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[dhcpserver] Oueries value: c7d49d7cecdc}[queryadaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[disableadapterdomainname] Oueries value:

```
c7d49d7cecdc}[registrationenabled]
     Oueries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-a
 c7d49d7cecdc}[registeradaptername]
     Oueries value:
c7d49d7cecdc}[registrationmaxaddresscount]
     Oueries value:
c7d49d7cecdc}[maxnumberofaddressestoregister]
     Oueries value:
c7d49d7cecdc}[domain]
     Oueries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-a
c7d49d7cecdc}[dhcpdomain]
                                                                     HKLM\software\microsoft\rpc\securityservice[10]
     Oueries value:
     Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
     Oueries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-a
c7d49d7cecdc}[ipautoconfigurationenabled]
                                                                    {\tt HKLM \ } system \verb| current control set \verb| control \ \\ session
     Oueries value:
manager[safeprocesssearchmode]
     Queries value:
                                                                    HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
     Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]
     Queries value:
c7d49d7cecdc}[addresstype]
     Oueries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-4404, and the services \ tcpip \ parameters \ terrange \ terr
c7d49d7cecdc}[nameserver]
     Queries value:
c7d49d7cecdc}[dhcpnameserver]
                                                                    HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
     Oueries value:
     Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]
                                                                    HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]
     Queries value:
     Oueries 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\digest.dll[name]
     Queries value:
     Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
                                                                    HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]
     Oueries value:
     Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities]
                                                                     HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid]
     Oueries value:
     Queries value:
                                                                     HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version]
                                                                     HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]
     Queries value:
     Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize]
     Queries value:
                                                                    HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
 cryptographic provider[type]
                                                                     HKLM \ software \ microsoft \ strong
     Queries value:
 cryptographic provider[image path]
     Queries value:
                                                                    HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name]
     Oueries value:
                                                                    HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment]
     Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities]
                                                                     HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid]
     Queries value:
                                                                     HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version]
     Oueries value:
     Queries value:
                                                                     HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type]
     Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize]
                                                                     HKLM\software\microsoft\cryptography[machineguid]
     Oueries value:
                                                                     \label{lem:hklm} \verb+Kklm \+ software \+ microsoft \+ rpc \+ security service \+ [default authlevel]
     Queries value:
                                                                     HKLM\system\currentcontrolset\services\winsock\parameters[transports]
     Oueries value:
     Oueries value:
                                                                     HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
     Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
     Oueries value:
```

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]

HKLM\software\microsoft\cryptography\rng[seed]

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]

Value changes: Value changes:

Oueries value:

 $\label{thm:local-soft-windows} Label{thm:local-windows} where $$\operatorname{ff90255c2-6bc4-11e3-9fc7-806d6172696f}[baseclass]$$

 $\label{thm:condition} \mbox{\currentversion} \mbox{\currentversion$

folders[cache]

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

folders[cookies]

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

folders[history]

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

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]