Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 8, Task ID: 19

Task ID: 19 Risk Level: 10

Date Processed: 2016-03-14 02:39:07 (UTC)

Processing Time: 61.9 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\spyeye_injector.exe"

Sample ID: 8
Type: basic
Owner: admin

Label: spyeye_injector.exe
Date Added: 2016-03-14 02:39:07 (UTC)

File Type: PE32:win32:gui File Size: PE32:win32:gui

MD5: b98bb6d7428c3dbffcfcab2414c6daa2

SHA256: fc7f54ce456c164452d8429a7fd5f52629a69338f8954e287d2664c03c37e029

Description: None

Pattern Matching Results

5 Abnormal sleep detected

- 5 Adds autostart object
- 4 Reads process memory
- 10 Suspicious writeprocess: Spyeye [Banking]
- 3 Program causes a crash [Info]
- 4 Terminates process under Windows subfolder
- 10 Creates malicious mutex: Spyeye [Banking]
- 6 Modifies registry autorun entries
- 6 Renames file on boot
- Writes to memory of system processes
- 3 Connects to local host
- 5 PE: Contains compressed section
- 6 Notifies system about Internet connection change
- 5 Packer: UPX
- 2 PE: Nonstandard section
- 3 HTTP connection response code 200 (success)

Static Events

Anomaly: PE: Contains a virtual section
Anomaly: PE: Contains one or more non-standard sections
Packer: UPX

Process/Thread Events

Creates process: C:\windows\temp\spyeye_injector.exe

["C:\windows\temp\spyeye_injector.exe"]

Creates process: C:\WinOldFileq\83A49421CBD.exe ["C:\WinOldFileq\83A49421CBD.exe"]

Creates process: C:\Users\Admin\AppData\Local\Temp\SIm8C5.exe

["C:\Users\Admin\AppData\Local\Temp\SIm8C5.exe"]

Creates process: C:\Windows\SysWOW64\rundll32.exe ["C:\Windows\system32\rundll32.exe""C:\Windows\syswow64\WININET.dll",DispatchAPICall 1]

Reads from process: PID:1040 C:\Windows\explorer.exe Reads from process: PID:348 C:\Windows\System32\wininit.exe PID:388 C:\Windows\System32\winlogon.exe Reads from process: Reads from process: PID:460 C:\Windows\System32\lsass.exe Reads from process: PID:468 C:\Windows\System32\lsm.exe PID:572 C:\Windows\System32\svchost.exe Reads from process: Reads from process: PID:640 C:\Windows\System32\svchost.exe Reads from process: PID:692 C:\Windows\System32\svchost.exe PID:800 C:\Windows\System32\svchost.exe Reads from process: Reads from process: PID:852 C:\Windows\System32\svchost.exe Reads from process: PID:940 C:\Windows\System32\svchost.exe Reads from process: PID:260 C:\Windows\System32\dwm.exe Reads from process:

Reads from process: PID:260 C:\Windows\System32\dwm.exe
Reads from process: PID:1048 C:\Windows\System32\spoolsv.exe
Reads from process: PID:1120 C:\Windows\System32\svchost.exe
Reads from process: PID:1128 C:\Windows\System32\svchost.exe
Reads from process: PID:1340 C:\Windows\System32\svchost.exe
Reads from process: PID:1404 C:\Windows\System32\svchost.exe
Reads from process: PID:1812 C:\Windows\System32\svchost.exe
Reads from process: PID:1964 C:\Windows\System32\svchost.exe
Reads from process: PID:1732 C:\Windows\System32\svchost.exe
Reads from process: PID:1732 C:\Windows\System32\svchost.exe

Reads from process: PID:1848 C:\Windows\\$ystem32\rundll32.exe
Reads from process: PID:1884 C:\Windows\\$ystem32\rundll32.exe
Reads from process: PID:1864 C:\Windows\\$ystem32\sdclt.exe
Reads from process: PID:1740 C:\Windows\\$ystem32\taskhost.exe
Reads from process: PID:1624 C:\Windows\\$ystem32\taskhost.exe

Reads from process: PID:2412 C:\Windows\System32\WinSAT.exe
Reads from process: PID:2420 C:\Windows\System32\conhost.exe

```
Reads from process:
                         PID:2432 C:\Windows\System32\wbem\unsecapp.exe
                         PID:2496 C:\Windows\System32\wbem\WmiPrvSE.exe
Reads from process:
Reads from process:
                         PID:2568 C:\Windows\System32\conhost.exe
Reads from process:
                         PID:2812 C:\Windows\System32\schtasks.exe
                         PID:1300 C:\Program Files (x86)\Adobe\Reader 9.0\Reader\reader_sl.exe
Writes to process:
Writes to process:
                         PID:2660 C:\Users\Admin\AppData\Local\Temp\SIm8C5.exe
                         PID:2896 C:\Windows\SysWOW64\rundll32.exe
Writes to process:
                         PID:2992 C:\Windows\SysWOW64\WerFault.exe
Writes to process:
Writes to process:
                         PID:2056 C:\Windows\SysWOW64\rundll32.exe
Writes to process:
                         PID:2080 C:\Windows\SysWOW64\rundll32.exe
                         PID:2132 C:\Windows\SysWOW64\WerFault.exe
Writes to process:
Writes to process:
                         PID:2252 C:\Windows\SysWOW64\rundll32.exe
Writes to process:
                         PID:2304 C:\Windows\SysWOW64\rundll32.exe
                         PID:2300 C:\Windows\SysWOW64\WerFault.exe
Writes to process:
Writes to process:
                         PID:364 C:\Windows\SysWOW64\rundll32.exe
Writes to process:
                         PID:2332 C:\Windows\SysWOW64\WerFault.exe
                         PID:2360 C:\Windows\SysWOW64\rundll32.exe
Writes to process:
Writes to process:
                         PID:2344 C:\Windows\SysWOW64\WerFault.exe
Terminates process:
                         C:\WinOldFileq\83A49421CBD.exe
                         C:\Windows\Temp\spyeye_injector.exe
Terminates process:
Terminates process:
                         C:\Windows\SysWOW64\WerFault.exe
Terminates process:
                         C:\Windows\SysWOW64\rundll32.exe
```

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\BaseNamedObjects\RPCController
Creates mutex:	\Sessions\1\BaseNamedObjects\zXeRY3a_PtW 0000000
Creates mutex:	\BaseNamedObjects\Yy05UQIWGSu5MCKMS7WyU05SC5kOqSC
Creates mutex:	\Sessions\1\BaseNamedObjects_!MSFTHISTORY!_
Creates mutex:	

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!temporary internet files!content.ie5!

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!roaming!microsoft!windows!cookies!

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!history!history.ie5!

Creates mutex: \Sessions\1\BaseNamedObjects\WininetStartupMutex $\verb|\Sessions|1\BaseNamedObjects|\WininetConnectionMutex|$ Creates mutex: Creates mutex: \Sessions\1\BaseNamedObjects\WininetProxyRegistryMutex

\Sessions\1\BaseNamedObjects\RasPbFile Creates mutex:

\Sessions\1\BaseNamedObjects\ZonesCounterMutex Creates mutex:

Creates mutex: \Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex

Creates mutex: \Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex $\verb|\Sessions|1\BaseNamedObjects|\ZonesLockedCacheCounterMutex|$ Creates mutex:

Creates mutex: \Sessions\1\BaseNamedObjects\!IETld!Mutex

Creates mutex: \Sessions\1\BaseNamedObjects_!MSFTHISTORY!_LOW!_

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!temporary internet files!low!content.ie5!

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!roaming!microsoft!windows!cookies!low! Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!history!low!history.ie5!

Creates event: \BaseNamedObjects\SvcctrlStartEvent_A3752DX Creates event: \Security\LSA_AUTHENTICATION_INITIALIZED Creates event: \KernelObjects\SystemErrorPortReady

Creates event: \BaseNamedObjects\BFE_Notify_Event_{8bf8c154-c669-4ac4-b7eb-

e9a100dc15aa}

File System Events		
Creates:	C:\WinOldFileq	
Creates:	C:\WinOldFileq\	
Creates:	C:\WinOldFileq\83A49421CBD.exe	
Creates:	C:\WinOldFileq\8FDC7C717274206	
Creates:	<pre>C:\Users\Admin\AppData\Local\Temp\</pre>	
Creates:	<pre>C:\Users\Admin\AppData\Local\Temp\SIm8C5.tmp</pre>	
Creates:	<pre>C:\Users\Admin\AppData\Local\Temp\SIm8C5.exe</pre>	
Creates:	C:\Users\Admin	
Creates:	C:\Users\Admin\AppData\Local	
Creates:	<pre>C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files</pre>	
Creates:	<pre>C:\Users\Admin\AppData\Roaming</pre>	
Creates:	<pre>C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies</pre>	
Creates:	<pre>C:\Users\Admin\AppData\Local\Microsoft\Windows\History</pre>	
Creates:	C:\Users\Admin\Favorites	
Creates:	<pre>C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE</pre>	
Creates:	<pre>C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache</pre>	
Creates:	<pre>C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache</pre>	
Opens:	<pre>C:\Windows\Prefetch\SPYEYE_INJECTOR.EXE-619282B0.pf</pre>	
Onens:	C:\Windows	

Opens: C:\Windows

C:\Windows\System32\wow64.dll Opens: C:\Windows\System32\wow64win.dll Opens: Opens: C:\Windows\System32\wow64cpu.dll

```
Opens:
                         C:\Windows\system32\wow64log.dll
 Opens:
                         C:\Windows\SvsWOW64
                         C:\Windows\SysWOW64\sechost.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\kernel32.dll
 Opens:
                         C:\
 Opens:
                         C:\Windows\Globalization\Sorting\SortDefault.nls
                         C:\Windows\SysWOW64\ntdll.dll
 Opens:
 Opens:
                         C:\WinOldFilea
 Opens:
                         C:\WinOldFileq\
                         C:\Windows\Temp\spyeye_injector.exe
 Opens:
 Opens:
                         C:\WinOldFileq\83A49421CBD.exe
 Opens:
                         C:\Windows\SysWOW64\apphelp.dll
 Opens:
                         C:\Windows\AppPatch\sysmain.sdb
 Opens:
                         C:\WinOldFileq\ui\SwDRM.dll
                         C:\Windows\Prefetch\83A49421CBD.EXE-8B5C1E36.pf
 Opens:
                         C:\Windows\SysWOW64\imm32.dll
 Opens:
 Opens:
                         C:\WinOldFileq\MSIMG32.dll
 Opens:
                         C:\Windows\SysWOW64\msimg32.dll
 Opens:
                         C:\WinOldFileq\8FDC7C717274206
 Opens:
                         C:\Users\Admin\AppData\Local\Temp
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\SIm8C5.exe
 Opens:
                         C:\Users
 Opens:
                         C:\Users\Admin
 Opens:
                         C:\Users\Admin\AppData
 Opens:
                         C:\Users\Admin\AppData\Local
                         C:\Users\Admin\AppData\Local\Temp\ui\SwDRM.dll
 Opens:
 Opens:
                         C:\Windows\Prefetch\SIM8C5.EXE-6FF38363.pf
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\MSIMG32.dll
                         C:\Windows\SysWOW64\user32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\wininet.dll
 Opens:
                         C:\Windows\SysWOW64\ws2_32.dll
                         C:\Windows\SysWOW64\advapi32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\crypt32.dll
 Opens:
                         C:\Windows\SysWOW64\tzres.dll
 Opens:
                         C:\Windows\SysWOW64\en-US\tzres.dll.mui
 Opens:
                         C:\windows\temp\spyeye_injector.exe
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\SIm8C5.exe.Local\
                         C:\Windows\winsxs\x86_microsoft.windows.common-
 Opens:
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
                         C:\Windows\winsxs\x86_microsoft.windows.common-
 Opens:
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
                         C:\Windows\WindowsShell.Manifest
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\USERENV.dll
                         C:\Windows\SysWOW64\userenv.dll
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\profapi.dll
 Opens:
                         C:\Windows\SysWOW64\profapi.dll
 Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates
                         C:\Windows\SysWOW64\mswsock.dll
 Opens:
                         C: \verb|\USers\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs|
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\desktop.ini
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\desktop.ini
                         C:\Users\Admin\AppData\Roaming
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History
 Opens:
                         C: \verb|\USers\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini|
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
 Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5\index.dat
                         \verb|C:\USers\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat|\\
 Opens:
 Opens:
\verb|C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\Index.dat| \\
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\dnsapi.DLL
 Opens:
                         C:\Windows\SysWOW64\dnsapi.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\iphlpapi.DLL
                         C:\Windows\SysWOW64\IPHLPAPI.DLL
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\WINNSI.DLL
 Opens:
                         C:\Windows\SysWOW64\winnsi.dll
 Opens:
                         C:\Windows\SysWOW64\WSHTCPIP.DLL
 Opens:
                         C:\Program Files (x86)\Adobe\Reader 9.0\Reader\MSIMG32.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\RASAPI32.dll
 Opens:
                         C:\Windows\SysWOW64\rasapi32.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\rasman.dll
                         C:\Windows\SysWOW64\rasman.dll
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\rtutils.dll
```

```
C:\Windows\SysWOW64\rtutils.dll
  Opens:
  Opens:
                                       C:\ProgramData\Microsoft\Network\Connections\Pbk\
  Opens:
                                       C:\Windows\SysWOW64\ras
  Opens:
                                       C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk
  Opens:
                                       C:\Users\Admin\AppData\Local\Temp\sensapi.dll
  Opens:
                                       C:\Windows\SysWOW64\SensApi.dll
                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\Low
  Opens:
                                       C:\Users\Admin\AppData\Local\Microsoft\Windows
  Opens:
                                       C:\Users\Admin\AppData\Local\Microsoft
  Opens:
                                       C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\Low
  Opens:
                                       C:\Users\Admin\AppData\Roaming\Microsoft\Windows
  Opens:
                                       C:\Users\Admin\AppData\Roaming\Microsoft
  Opens:
                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low
  Opens:
                                       C:\Users\Admin\Favorites
                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\Virtualized
  Opens:
                                       C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE
  Opens:
                                       C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE\Low
                                       {\tt C: \tt Vsers \tt Admin \tt AppData \tt Roaming \tt Microsoft \tt Windows \tt IECompatCache}
  Opens:
                                       C: \verb|VarsAdminAppDataRoamingMicrosoftWindows\| IECompatCache \verb|Low| | IECompatCache | IEC
  Opens:
                                       C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache
  Opens:
  Opens:
                                       C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache\Low
  Opens:
                                       C:\Users\Admin\AppData\Local\Temp\Low
  Opens:
                                       C:\Windows\SysWOW64\rundll32.exe
  Opens:
                                       C:\Windows\SysWOW64\ui\SwDRM.dll
  Opens:
                                       C:\Windows\SysWOW64\nlaapi.dll
  Opens:
                                       C:\Windows\Prefetch\RUNDLL32.EXE-87432CEE.pf
  Opens:
                                       C:\Users\Admin\AppData\Local\Temp\rasadhlp.dll
  Opens:
                                       C:\Windows\SysWOW64\rasadhlp.dll
  Opens:
                                       C:\Windows\SysWOW64\uxtheme.dll
  Opens:
                                       C:\Users\Admin\AppData\Local\Temp\wkscli.dll
  Opens:
                                       C:\Windows\SysWOW64\wkscli.dll
  Opens:
                                       C:\Users\Admin\AppData\Local\Temp\netutils.dll
  Opens:
                                       C:\Windows\SysWOW64\netutils.dll
  Opens:
                                       C:\Windows\SysWOW64\wship6.dll
  Opens:
                                       C:\Users\Admin\AppData\Local\Temp\dhcpcsvc6.DLL
  Opens:
                                       C:\Windows\SysWOW64\dhcpcsvc6.dll
  Opens:
                                       C:\Users\Admin\AppData\Local\Temp\dhcpcsvc.DLL
  Opens:
                                       C:\Windows\SysWOW64\dhcpcsvc.dll
  Opens:
                                       C:\Windows\System32\drivers\etc\hosts
  Opens:
                                       C:\Windows\SysWOW64\FWPUCLNT.DLL
  Opens:
                                       C:\Windows\SysWOW64\NapiNSP.dll
                                       C:\Windows\SysWOW64\pnrpnsp.dll
  Opens:
  Opens:
                                       C:\Windows\SysWOW64\winrnr.dll
  Opens:
                                       C:\Users\Admin\AppData\Local\Temp\ntmarta.dll
  Opens:
                                       C:\Windows\SysWOW64\ntmarta.dll
  Opens:
                                       C:\Users\Admin\AppData\Local\Temp\VERSION.dll
  Opens:
                                       C:\Windows\SysWOW64\version.dll
  Opens:
                                       C:\Windows\SysWOW64\en-US\urlmon.dll.mui
  Opens:
                                       C:\Windows\Prefetch\WERFAULT.EXE-37549B7E.pf
  Opens:
                                       C:\Windows\AppPatch\AcLayers.dll
  Opens:
                                       C:\Windows\SysWOW64\winspool.drv
  Opens:
                                       C:\Windows\SysWOW64\mpr.dll
  Opens:
                                       C:\Windows\AppPatch\acwow64.dll
                                       C:\Windows\SysWOW64\en-US\rundll32.exe.mui
  Opens:
  Opens:
                                       C:\Windows\syswow64\WININET.dll.manifest
                                       C:\Windows\SysWOW64\dwmapi.dll
  Opens:
                                       C:\Windows\SysWOW64\rundll32.exe.Local\
  Opens:
  Opens:
                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low\desktop.ini
  Opens:
                                       {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Low\Content.IE5
                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\Low\Content.IE5\desktop.ini
                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\desktop.ini
  Opens:
  Opens:
                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\History.IE5
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\History.IE5\desktop.ini
                                       C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\Low\Content.IE5\index.dat
                                       C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\Low\index.dat
  Opens:
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\History.IE5\index.dat
  Writes to:
                                       C:\WinOldFileq\83A49421CBD.exe
                                       C:\WinOldFileq\8FDC7C717274206
  Writes to:
  Writes to:
                                       C:\Users\Admin\AppData\Local\Temp\SIm8C5.exe
  Reads from:
                                       C:\Windows\SysWOW64\ntdll.dll
  Reads from:
                                       C:\Windows\Temp\spyeye_injector.exe
  Reads from:
                                       C:\WinOldFileq\83A49421CBD.exe
```

Reads from: C:\Users\Admin\AppData\Local\Temp\SIm8C5.exe
Reads from: C:\Windows\SysWOW64\user32.dl1

C:\WinOldFileq\8FDC7C717274206

Reads from:

Reads from: C:\Windows\SysWOW64\wininet.dll
Reads from: C:\Windows\SysWOW64\ws2_32.dll
Reads from: C:\Windows\SysWOW64\advapi32.dll
Reads from: C:\Windows\SysWOW64\crypt32.dll
Reads from: C:\Windows\SysWOW64\rundll32.exe
Reads from: C:\Windows\SysWOW64\rundll32.exe
Reads from: C:\Windows\System32\drivers\etc\hosts
Deletes: C:\Windows\Temp\spyeye_injector.exe

Network Events

DNS query: alexeyartemov.com DNS query: www.microsoft.com DNS response: alexeyartemov.com \Rightarrow 198.105.244.11 DNS response: alexeyartemov.com \Rightarrow 104.239.213.7 e10088.dspb.akamaiedge.net ⇒ 23.15.109.88 e10088.dspb.akamaiedge.net ⇒ 173.223.40.170 DNS response: DNS response: DNS response: e10088.dspb.akamaiedge.net ⇒ 23.193.127.198 e10088.dspb.akamaiedge.net ⇒ 23.211.115.218 DNS response: 88.198.13.147:443 Connects to: Connects to: 104.239.213.7:80 Connects to: 0.0.0.0:80 127.0.0.1:80 Connects to: Connects to: 23.15.109.88:80 173.223.40.170:80 Connects to: Connects to: 198.105.244.11:80 Sends data to: 8.8.8.8:53 Sends data to: 4.2.2.1:53 alexeyartemov.com:80 (104.239.213.7) Sends data to: Sends data to: e10088.dspb.akamaiedge.net:80 (23.15.109.88) Sends data to: e10088.dspb.akamaiedge.net:80 (173.223.40.170) Sends data to: alexeyartemov.com:80 (198.105.244.11) Receives data from: 8.8.8.8:53 Receives data from: 4.2.2.1:53 Receives data from: alexeyartemov.com:80 (104.239.213.7) Receives data from: e10088.dspb.akamaiedge.net:80 (23.15.109.88) Receives data from: e10088.dspb.akamaiedge.net:80 (173.223.40.170) Receives data from: alexeyartemov.com:80 (198.105.244.11)

Windows Registry Events

Creates key:	HKLM\system\currentcontrolset\control\session manager
Creates key:	HKCU\software\microsoft\windows\currentversion\run
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings</pre>
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
Creates key:	HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_	zones\1
Creates key:	HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_	zones\2
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>
settings\lockdown_	zones\3
Creates key:	HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_	zones\4
Creates key:	<pre>HKCU\software\microsoft\internet explorer\phishingfilter</pre>
Creates key:	HKCU\software\microsoft\internet explorer\recovery
Creates key:	HKCU\software\microsoft\systemcertificates\my
Creates key:	HKLM\software\wow6432node\microsoft\tracing
Creates key:	<pre>HKLM\software\wow6432node\microsoft\tracing\sim8c5_rasapi32</pre>
Creates key:	<pre>HKLM\software\wow6432node\microsoft\tracing\sim8c5_rasmancs</pre>
Creates key:	HKCU\software\microsoft windows
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>
settings\connectio	ns
Creates key:	HKCU\software\appdatalow
Creates key:	HKCU\software\microsoft\internet explorer\internetregistry
Creates key:	<pre>HKCU\software\microsoft\internet explorer\lowregistry</pre>
Creates key:	HKCU\software\microsoft\internet
explorer\lowregist	ry\dontshowmethisdialogagain
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>
settings\5.0\lowca	che
Creates key:	<pre>HKCU\software\microsoft\internet explorer\intelliforms</pre>
Creates key:	<pre>HKCU\software\microsoft\internet explorer\toolbar</pre>
Creates key:	<pre>HKCU\software\microsoft\internet explorer\toolbar\webbrowser</pre>
Creates key:	
HKCU\software\micr	osoft\windows\currentversion\explorer\menuorder\favorites
Creates key:	<pre>HKCU\software\microsoft\internet explorer\pagesetup</pre>
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>
settings\passport\	lowdamap
	LIKCUS - Channel Stranger Channel Chan

Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\lowregistry
Creates key: HKCU\software\microsoft\internet explorer\zoom
Creates key: HKCU\software\microsoft\internet explorer\browseremulation\lowmic

Creates key: HKCU\software\microsoft\internet explorer\ietld\lowmic

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

awareness

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

settings\p3p\history

Creates key: HKLM\software\wow6432node

Creates key: HKLM\software\wow6432node\microsoft

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]

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

settings\zonemap[proxybypass]

Deletes value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\zonemap[proxybypass]

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

settings\zonemap[intranetname]

Deletes value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\zonemap[intranetname]

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

options

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

Opens key: HKLM\software\microsoft\wow64

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file

execution options

Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll

Opens key:

 $HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ safer \ code identifiers$

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

Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\language
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us

Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete

Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings

Opens key: HKLM\software\policies\microsoft\mui\settings

Opens key: HKCU\

Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKLM\system\currentcontrol\set\control\mui\settings\languageconfiguration

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

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

 $Opens~key: \\ HKLM \software \wow 6432 node \microsoft \windows \current version \side by side \\$

Opens key: HKLM\

Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\diagnostics

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

Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername

Opens key: HKLM\system\setup

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

options\83a49421cbd.exe

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

 $Opens~key: \\ HKLM\software\wow6432node\policies\microsoft\windows\appcompat$

Opens key: HKLM\software\policies\microsoft\windows\appcompat

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers

 $\label{lem:constraint} Opens \ key: \\ HKLM \ software \ microsoft \ windows \\ nt \ current version \ app compatflags \ custom \ 83a49421cbd.exe$

Opens key: HKLM\system\currentcontrolset\services\crypt32

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file

execution options\83a49421cbd.exe

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

Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\appcompatflags

Opens key: HKLM\software\wow6432node\microsoft\windows

 $nt\current version\app compatflags\custom\83a49421cbd.exe$

Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\gre_initialize

Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\compatibility32

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime

compatibility

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows

Opens key: HKLM\software\wow6432node\microsoft\ole

Opens key: HKLM\software\wow6432node\microsoft\ole\tracing

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

HKLM\software\wow6432node\microsoft\oleaut Opens key:

Opens key:

settings Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

settings

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

options\sim8c5.exe

HKLM\software\microsoft\windows Opens key: nt\currentversion\appcompatflags\custom\sim8c5.exe

Opens key: HKLM\software\wow6432node\microsoft\internet explorer

HKCU\software\microsoft\windows\currentversion\internet settings\user Opens kev:

agent

Opens key:

settings\user agent

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

settings\5.0\user agent

HKLM\software\wow6432node\microsoft\windows\currentversion\internet Opens kev:

settings\5.0\user agent

Opens key: HKLM\software\wow6432node\policies

HKCU\software\policies Opens key: Opens key: HKCU\software Opens key: HKLM\software\wow6432node

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

settings\user agent

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

settings

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

settings\user agent

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\user agent\ua tokens HKCU\software\microsoft\windows\currentversion\internet settings Opens kev:

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\user agent\pre platform

HKLM\software\wow6432node\microsoft\windows\currentversion\internet Opens key:

settings\5.0\user agent\pre platform

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

settings\5.0\user agent\pre platform

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\user agent\post platform

HKLM\software\wow6432node\microsoft\windows\currentversion\internet Opens key:

settings\5.0\user agent\post platform

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

settings\5.0\user agent\post platform

Opens key: HKLM\system\currentcontrolset\control\cmf\config

Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr

Opens key: HKLM\software\wow6432node\policies\microsoft\internet

explorer\main\featurecontrol

Opens key: $\label{lem:hklm} \verb+Kklm \+ software \+ policies \+ microsoft \+ internet explorer \+ main \+ feature control$ HKCU\software\policies\microsoft\internet explorer\main\featurecontrol Opens kev:

Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol

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

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

Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_browser_emulation

HKLM\software\policies\microsoft\sqmclient\windows Opens key:

Opens kev: HKLM\software\microsoft\samclient\windows

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters

HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog Opens kev:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\33ea8657

Opens key:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005

Opens kev:

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003

Opens key:

Opens key:

```
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
   Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
   Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000003
                                              HKLM\software\wow6432node\policies\microsoft\internet explorer
   Opens key:
   Opens key:
                                              HKLM\software\policies\microsoft\internet explorer
   Opens key:
                                              HKLM\software\wow6432node\policies\microsoft\internet explorer\main
                                              HKLM\software\policies\microsoft\internet explorer\main
   Opens key:
   Opens key:
                                              HKLM\software\wow6432node\microsoft\cryptography\oid
   Opens key:
                                              HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 0
                                              HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
   Opens key:
0\certdllopenstoreprov
   Opens key:
                                              HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov\#16
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
   Opens key:
                                              HKLM\software\wow6432node\microsoft\rpc
   Opens key:
Opens key:
                                              HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
   Opens key:
                                              HKLM\software\policies\microsoft\windows nt\rpc
                                              HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
   Opens kev:
0\certdllopenstoreprov\ldap
                                              HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 1
   Opens kev:
   Opens key:
                                              HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
1\certdllopenstoreprov
   Opens key:
                                              HKCU\software\microsoft\systemcertificates\my\physicalstores
   Opens kev:
   Opens key:
HKLM\software\wow6432node\microsoft\windows
   Opens kev:
nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001
   Opens key:
                                              \label{lem:hklm} \mbox{ HKLM} \mbox{ hicrosoft} \mbox{ in \current version \profile list \s-1-5-21-1} \mbox{ list} \mbox
980053277-1733835069-2361817685-1001
   Opens key:
                                             HKCU\software\microsoft\systemcertificates\my
   Opens key:
                                              HKCU\software\microsoft\systemcertificates\my\
                                              \begin{tabular}{ll} HKCU \label{limits} & \textbf{KCU} \end{tabular} is a time that $$ \textbf{KCU} \end{tabular} is a time that $$\textbf{KCU} \end{tabular} is a time that $$ \textbf{KCU} \end{ta
   Opens key:
                                              HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
   Opens key:
settings\5.0\cache
  Opens key:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
                                              HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\5.0\cache\content
   Opens key:
                                              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\content
   Opens key:
                                              HKCU\software\microsoft\systemcertificates\my\crls
   Opens key:
                                              \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \systemcertificates \verb+my \ctls+ \\
   Opens key:
                                              HKCU\software\microsoft\systemcertificates\my\keys
   Opens kev:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ \ folder descriptions
33be-4251-ba85-6007caedcf9d}
   Opens key:
33be-4251-ba85-6007caedcf9d}\propertybag
   Opens key:
                                              HKCU\software\microsoft\windows\currentversion\explorer
   Opens key:
                                              HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
```

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

Opens key: folders

Opens key:

Opens key: HKLM\software\wow6432node\policies\microsoft\windows\explorer Opens key: HKLM\software\policies\microsoft\windows\explorer Opens key: HKCU\software\policies\microsoft\windows\explorer Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f1b32785-b2785$ 6fba-4fcf-9d55-7b8e7f157091}

Opens kev:

6fba-4fcf-9d55-7b8e7f157091}\propertybag

Opens key:

0e22-4760-9afe-ea3317b67173}

Opens key:

0e22-4760-9afe-ea3317b67173}\propertybag

Opens key:

 $HKLM \setminus software \setminus wow6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus known folders \\ ettings$

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

settings\5.0\cache\cookies

HKLM\software\wow6432node\microsoft\windows\currentversion\internet Opens key:

settings\5.0\cache\cookies

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-16444, 2b0f765d-16444, 2b0f766d-16444, 2b0f76d-16444, 2b0f76d-16444$ c0e9-4171-908e-08a611b84ff6}

Opens key:

 $HKLM \label{lem:hklm} White the latest and the la$ c0e9-4171-908e-08a611b84ff6}\propertybag

Opens key:

65f9-4cf6-a03a-e3ef65729f3d}

Opens kev:

65f9-4cf6-a03a-e3ef65729f3d}\propertybag

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

settings\5.0\cache\history

HKLM\software\wow6432node\microsoft\windows\currentversion\internet Opens key:

settings\5.0\cache\history

Opens key:

b784-432e-a781-5a1130a75963}

Opens key:

b784-432e-a781-5a1130a75963}\propertybag

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

settings\5.0\cache\extensible cache

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

settings\5.0\cache\extensible cache\domstore

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

settings\5.0\cache\extensible cache\feedplat

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

settings\5.0\cache\extensible cache\iecompat HKCU\software\microsoft\windows\currentversion\internet Opens kev:

settings\5.0\cache\extensible cache\ietld

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

settings\5.0\cache\extensible cache\privacie:

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_bufferbreaking_818408

Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_bufferbreaking_818408 Opens kev: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954

HKLM\software\wow6432node\microsoft\internet Opens kev:

explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954

Opens key:

 $HKLM \backslash software \backslash wow 6432 node \backslash policies \backslash microsoft \backslash windows \backslash current version \backslash internet settings \backslash 5.0 \backslash cache$ HKLM\software\policies\microsoft\windows\currentversion\internet Opens kev:

settings\5.0\cache

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

settings\5.0\cache

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289

Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289

HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266

```
HKLM\software\wow6432node\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature disable notify unverified spn kb2385266
   Opens kev:
                                             HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
   Opens kev:
                                             HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
                                             HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_allow_long_international_filenames
   Opens key:
                                             HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
   Opens kev:
                                             HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
   Opens key:
                                             HKLM\software\wow6432node\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
                                             HKLM\software\wow6432node\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
   Opens key:
                                             HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
   Opens key:
                                             HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
   Opens kev:
                                             HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
   Opens key:
                                             HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
   Opens key:
                                             HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
                                             HKCU\software\microsoft\internet
   Opens kev:
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
   Opens key:
                                             HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
   Opens key:
                                             HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
   Opens key:
                                             HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
   Opens key:
                                             HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
                                             HKLM\software\wow6432node\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
                                             HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
   Opens key:
                                            HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
   Opens key:
                                             HKCU\software\microsoft\windows\currentversion\internet settings\wpad
   Opens key:
                                             HKLM\system\currentcontrolset\services\winsock\parameters
                                             HKLM \verb|\system| current controlset \verb|\services| tcpip6 \verb|\parameters| winsock
   Opens key:
   Opens key:
                                             \label{lem:hklm} \verb+Kklm \system \current control set \services \tcpip \parameters \winsock
                                             HKLM\system\currentcontrolset\services\winsock\setup migration\providers
   Opens kev:
                                             Opens key:
migration\providers\tcpip
                                             HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
   Opens key:
                                             HKLM\software\wow6432node\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\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
   Opens key:
                                             HKLM\software\wow6432node\microsoft\tracing\sim8c5_rasapi32
   Opens key:
                                             HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist
   Opens key:
                                             HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
   Opens key:
                                             HKLM\software\microsoft\sqmclient\windows\disabledsessions\
   Opens key:
                                             HKLM \ software \ wow 6432 node \ microsoft \ tracing \ sim 8c5\_rasmancs
   Opens key:
                                             HKLM\system\currentcontrolset\control\sqmservicelist
   Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1777f761-16164, 1977f761-1616, 1977f761-1616
68ad-4d8a-87bd-30b759fa33dd}
   Opens key:
HKLM \label{lem:hklm} White the latest and the la
68ad-4d8a-87bd-30b759fa33dd}\propertybag
   Opens key:
                                             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe
   Opens key:
                                             HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\rundll32.exe
                                             \label{lem:hklm} \verb+Kklm \+ software \+ microsoft \+ windows nt \+ current version \+ app compatflags
   Opens key:
                                             HKCU\software\microsoft\windows nt\currentversion\appcompatflags
   Opens kev:
   Opens key:
                                             HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
   Opens key:
                                             HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
   Opens key:
                                             HKCU\software\microsoft\internet
```

```
explorer\main\featurecontrol\feature_mime_handling
                                                       HKLM\software\wow6432node\microsoft\internet
   Opens kev:
explorer\main\featurecontrol\feature_mime_handling
                                                        HKLM\system\currentcontrolset\services\dnscache\parameters
    Opens key:
    Opens key:
                                                        HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
    Opens key:
                                                        HKLM\software\policies\microsoft\windows nt\dnsclient
    Opens key:
                                                        HKLM\system\currentcontrolset\services\dns
                                                        HKLM\software\wow6432node\policies\microsoft\windows
    Opens key:
nt\dnsclient\dnspolicyconfig
    Opens key:
                                                        HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
    Opens kev:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
    Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\
    Opens key:
                                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
                                                        HKLM\software\wow6432node\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
    Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\zonemap\domains\
    Opens key:
                                                        HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains
    Opens key:
                                                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
   Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus microsoft \setminus micr
settings\zonemap\ranges\
                                                        HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\zonemap\ranges
   Opens key:
                                                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
                                                        HKCU\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_unc_savedfilecheck
                                                        HKLM\software\wow6432node\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_unc_savedfilecheck
   Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
                                                        HKCU\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
                                                        HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet
    Opens key:
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
   Opens kev:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap
                                                        HKLM\software\policies\microsoft\windows\currentversion\internet
    Opens kev:
settings\zonemap
    Opens key:
                                                        \label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\internet}}
settings\zonemap
                                                        HKCU\software\microsoft\windows\currentversion\internet
   Opens kev:
settings\zonemap\ranges\
                                                        HKCU\software\microsoft\windows\currentversion\internet
    Opens key:
settings\zonemap\protocoldefaults\
                                                        HKCU\software\microsoft\windows\currentversion\internet
    Opens key:
settings\zonemap\domains\
                                                        HKLM\software\wow6432node\microsoft\windows\currentversion\internet
   Opens kev:
settings\zonemap\domains\
    Opens key:
                                                        HKLM\software\policies\microsoft\internet explorer\security
    Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\internet settings\zones\
                                                        HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
    Opens key:
    Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
    Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
    Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
    Opens key:
                                                        \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\zones\4}}
    Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\
    Opens key:
                                                        HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones
   Opens key:
                                                        \label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\internet}}
settings\zones\
   Opens kev:
HKLM\software\policies\microsoft\windows\currentversion\internet
    Opens kev:
settings\zones\0
   Opens key:
                                                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
   Opens kev:
HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ current version \ internet\ settings \ 1000 node \ 1000 n
                                                        HKLM\software\policies\microsoft\windows\currentversion\internet
    Opens key:
settings\zones\1
   Opens key:
                                                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
   Opens key:
                                                        HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap\
```

```
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\2
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\2
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\zones\2
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\3
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\3
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\4
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\zones\4
                          HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
                          HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
 Opens kev:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\lockdown_zones\
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\0
 Opens key:
HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| windows\\| current version\\| internet
settings\lockdown_zones\0
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\0
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\0
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
 Opens kev:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\1
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\1
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
 Opens kev:
settings\lockdown_zones\2
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\2
 Opens key:
                          \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown zones\2
                          \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
 Opens key:
settings\lockdown_zones\3
 Opens key:
settings\lockdown_zones\3
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\3
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown zones\3
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\4
 Opens kev:
HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| windows\\| current version\\| internet
settings\lockdown_zones\4
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\4
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
 Opens key:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
 Opens key:
                          HKLM\software\policies\microsoft\windows\windows error reporting
 Opens key:
                          HKLM\software\microsoft\windows\windows error reporting
 Opens key:
                          HKLM\software\microsoft\windows\windows error reporting\debug
```

Opens key: HKCU\software\microsoft\windows\windows error reporting

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_zone_elevation

HKLM\software\wow6432node\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_zone_elevation

Opens key: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip6

Opens key: HKLM\software\wow6432node\policies\microsoft\system\dnsclient

Opens key: HKLM\software\policies\microsoft\system\dnsclient

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

Opens kev:

e1e01c1f69b5}

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}

Opens key:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{846ee342-7039-11de-9d20-

806e6f6e6963} Opens key:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-

806e6f6e69633 Opens key:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a91d0a5e-390e-4979-9c38-

127795cce47a} Opens key:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b9ec5865-2d36-4cb8-b474-

65fee5bae0b1}

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination $HKLM \verb|\system| current control \verb|\system| control contr$ Opens key:

Opens key: HKLM\system\currentcontrolset\services\ldap Opens key: HKCU\software\microsoft\internet explorer\ietld

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

settings\p3p\history\microsoft.com

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

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

settings\5.0\lowcache

HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\lowcache\content

Opens key:

HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\lowcache\cookies

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

settings\5.0\lowcache\history

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

settings\5.0\lowcache\extensible cache

 $\label{thm:linear} \mbox{HKCU\software\mbox{\sc urrentversion\internet}} \\$ Opens key: settings\5.0\lowcache\extensible cache\feedplat

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

settings\5.0\lowcache\extensible cache\iecompat

HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\lowcache\extensible cache\ietld

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

settings\5.0\lowcache\extensible cache\privacie:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\00f5af79-05320ef5

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\00f5af79 $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}$ Opens key:

settings\connections

HKLM\software\microsoft\windows nt\currentversion\image file execution Queries value:

options[disableusermodecallbackfilter]

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

manager[cwdillegalindllsearch]

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

Oueries value:

Oueries value:

 $HKLM \verb|\software| policies \verb|\microsoft| windows \verb|\safer| code identifiers[transparentenabled]|$ HKLM\system\currentcontrolset\control\nls\customlocale[empty] Oueries value:

HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]

Oueries value: HKLM\svstem\currentcontrolset\control\mui\uilanguages\en-us[type]

Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-

us[alternatecodepage]

Oueries value: HKCU\control panel\desktop[preferreduilanguages]

Oueries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]

Queries value:

Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]

Oueries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Oueries value: HKLM\system\currentcontrolset\control\computername\activecomputername[computername] Queries value: HKLM\system\setup[oobeinprogress] HKLM\system\setup[systemsetupinprogress] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cache] Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options[disablelocaloverride] HKLM\system\currentcontrolset\services\crypt32[debugheapflags] Oueries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles] HKLM\software\wow6432node\microsoft\windows Oueries value: nt\currentversion\compatibility32[83a49421cbd] HKLM\software\wow6432node\microsoft\windows Queries value: nt\currentversion\windows[loadappinit dlls] HKLM\software\microsoft\ole[pageallocatorusesystemheap] Queries value: Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[disableimprovedzonecheck] HKLM\software\policies\microsoft\windows\currentversion\internet Queries value: settings[security_hklm_only] HKLM\system\currentcontrolset\control\session Queries value: manager[pendingfilerenameoperations2] Oueries value: HKLM\system\currentcontrolset\control\session manager[pendingfilerenameoperations] HKLM\software\wow6432node\microsoft\windows Oueries value: nt\currentversion\compatibility32[sim8c5] HKLM\software\wow6432node\microsoft\internet explorer[version] Queries value: Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Queries value: settings\5.0\user agent[] $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ Queries value: settings\5.0\user agent[compatible] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Queries value: settings\5.0\user agent[compatible] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[version] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\user agent[version] HKCU\software\microsoft\windows\currentversion\internet settings[user Queries value: agent] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[platform] Queries value: settings\5.0\user agent[platform] HKLM\system\currentcontrolset\control\cmf\config[system] Oueries value: Queries value: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr[disable] HKLM\software\wow6432node\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_browser_emulation[sim8c5.exe] HKLM\software\wow6432node\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_browser_emulation[*] Oueries value: HKLM\software\microsoft\sqmclient\windows[ceipenable] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem] Queries value: $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ 0000000000003 \ [packed catalog item]$ Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem] Oueries value:

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries \ 0000000000007 \ [packed catalog item]$

Oueries value:

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000005[packedcatalogitem]

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]

Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000008[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem] Oueries value: Oueries value: $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ [serial_access_num]$ Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries] Oueries value: $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog \ (catalog_entries \ 00000000001[library path])$ Oueries value: $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ (catalog_entries \ 000000000001 \ [displaystring]$ Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily] Oueries 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\000000000001[enabled] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerinfo] Oueries 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] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[fromcachetimeout] Oueries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[secureprotocols] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000002[addressfamily] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled] HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version] Oueries value: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog5 \ catalog_entries \ 10000000000002 \ [storesservice class in fo]$ Oueries value: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000003[librarypath1 Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[secureprotocols] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[secureprotocols] Queries value: HKLM\system\currentcontrolset\services\crypt32[diaglevel] Oueries value: HKLM\system\currentcontrolset\services\crypt32[diagmatchanymask] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog 5 \setminus catalog_entries \setminus 0000000000003 [displaystring]$ Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[certificaterevocation] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[disablekeepalive] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablepassport] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[idnenabled] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog S \setminus catalog_entries \setminus 0000000000003[providerid]$ Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[addressfamily] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog 5 \setminus catalog_entries \setminus 0000000000003 [version]$

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

settings[cachemode]

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

settings[enablehttp1 11

Queries value: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}$

```
settings[enablehttp1_1]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablehttp1_1]
 Queries value:
                       HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
 Queries value:
                       \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
settings[proxyhttp1.1]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[proxyhttp1.1]
 Queries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
 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[disablebasicoverclearchannel]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_\catalog_entries\00000000003[storesserviceclassinfo]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog \\ \setminus catalog\_entries \setminus 0000000000003[provider info]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[librarypath]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus namespace\_catalog 5 \setminus catalog\_entries \setminus 0000000000004 [displaystring]
                       HKCU\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
                       HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
                       HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[clientauthbuiltinui]
                       HKLM\software\microsoft\rpc[maxrpcsize]
 Queries value:
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog S \setminus catalog\_entries \setminus 0000000000004 [providerid]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000004[supportednamespace]
 Oueries value:
Oueries value:
Queries value:
Oueries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace \_catalog5 \ catalog\_entries \ 000000000005 [library path]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
 Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[addressfamily]
 Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000005[supported name space]
 Queries value:
Oueries value:
Queries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[storesserviceclassinfo]
 Queries value:
Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ (catalog\_entries \ 000000000006 \ [library path]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog 5 \setminus catalog\_entries \setminus 0000000000006[displaystring]
                       HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
 Queries value:
980053277-1733835069-2361817685-1001[profileimagepath]
 Queries value:
                       HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
 Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[addressfamily]
 Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000006 [supported name space]]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[enabled]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
 Queries value:
```

Queries value:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[providerinfo]
                   HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[signature]
 Queries value:
                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
                   Queries value:
settings\5.0\cache\content[peruseritem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
 Queries value:
33be-4251-ba85-6007caedcf9d}[category]
 Queries value:
```

 $HKLM \\ software \\ \\ wow 6432 \\ node \\ microsoft \\ \\ windows \\ \\ current \\ version \\ \\ explorer \\ \\ folder \\ descriptions \\ \\ \{352481e8-33be-4251-ba85-6007 \\ caedcf9d \\ \\ [name]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ fgd \ [parent folder]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{352481e8-33be-4251-ba85-6007 caed \ folder \$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ folder \ f$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$

Oueries value:

 $\label{thm:local-condition} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdes$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ fgd \ [icon]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ fgd \ [security]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cal{lem:hklmsoftware} \end{substitute} 33be-4251-ba85-6007\caedcf9d\cal{lem:hklmsoftware} [streamresource]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ fgd \ [stream resource type]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ folder \ f$

Queries value:

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ fgd\} \ [stream]$

Queries value:

 $\label{thm:local-base-bound} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdes$

Queries value:

 $\label{thm:local-base-bound} HKLM \software \wow 6432 node \mbox{352481e8-33be-4251-ba85-6007} (attributes)$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cal{lem:hklmsoftware} \end{substitute} 33be-4251-ba85-6007\caedcf9d\cal{lem:hklmsoftware} [foldertypeid]$

Queries value:

 $\label{thm:local-base-bound} HKLM \software \wow 6432 node \mbox{352481e8-33be-4251-ba85-6007} [initfolder \mbox{handler}]$

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

folders[cache]

Queries value:

 $\label{lem:hkkm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\fifthed fib32785-6fba-4fcf-9d55-7b8e7f157091\fifthed fib2785-7b8e7f157091\fifthed f$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [name]$

Queries value:

 $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\fi1b32785-6fba-4fcf-9d55-7b8e7f157091\[parentfolder]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [relative path]$

Oueries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [parsing name]$

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [localized name]$

Oueries value:

 $\label{lem:hkkm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\fifthed folderdescriptions \fifthed folderdescriptions \fifthed$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [security]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [stream resource]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{fiba} $$Hklm \end{fiba} $$Hklm \end{fiba} $$ \end{fiba} $$ -4fcf-9d55-7b8e7f157091 \end{fiba} $$ \end{fiba} $$$ \end{fiba} $$ \end{fiba} $$ \end{fiba} $$ \end{fiba}$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{fiba} $$Hklm \end{fiba} $$Hklm \end{fiba} $$Hklm \end{fiba} $$157091 $$[local redirectonly] $$$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [precreate]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [stream]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [publish \ expanded \ path]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[attributes]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [folder type id]$

Queries value:

 $\label{thm:microsoftwindows} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\fifth 32785-66ba-4fcf-9d55-7b8e7f157091\fill\fifther]$

Queries value:

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

folders[local appdata]

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{area} Hklm \en$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [description]$

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{align*.} Hklm \end{ali$

Queries value

 $\label{thm:local-objective} HKLM \software \wow 6432 node \mbox{$5e6c858f-0e22-4760-9afe-ea3317b67173} [parsing name]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [infotip]$

Queries value:

 $\label{localized} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[localized name]}$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$

Queries value

 $\label{thm:local-software-wow6432} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$

Queries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f$

0e22-4760-9afe-ea3317b67173}[streamresourcetype]

0e22-4760-9afe-ea3317b67173}[localredirectonly]

Oueries value:

0e22-4760-9afe-ea3317b67173}[roamable]

Oueries value:

0e22-4760-9afe-ea3317b67173}[precreate]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[stream]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[publishexpandedpath]

Oueries value:

0e22-4760-9afe-ea3317b67173}[attributes]

Queries value:

0e22-4760-9afe-ea3317b67173}[foldertypeid]

Queries value:

0e22-4760-9afe-ea3317b67173}[initfolderhandler]

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

settings\5.0\cache\content[cacheprefix]

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

settings\5.0\cache\content[cachelimit]

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

settings\5.0\cache\cookies[peruseritem]

HKLM\software\wow6432node\microsoft\windows\currentversion\internet Queries value:

settings\5.0\cache\cookies[peruseritem]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765dc0e9-4171-908e-08a611b84ff6}[category]

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{2b0f765d-1644\} \\ folder \\ descriptions \setminus \{2b0f76d-1644\} \\ folder \\$ c0e9-4171-908e-08a611b84ff6}[name]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765dc0e9-4171-908e-08a611b84ff6}[parentfolder]

c0e9-4171-908e-08a611b84ff6}[description]

c0e9-4171-908e-08a611b84ff6}[relativepath] Oueries value:

HKLM\software\www6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765dc0e9-4171-908e-08a611b84ff6}[parsingname]

c0e9-4171-908e-08a611b84ff6}[infotip] Oueries value:

c0e9-4171-908e-08a611b84ff6}[localizedname]

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{2b0f765d-1644\} \\ folder \\ descriptions \setminus \{2b0f76d-1644\} \\ folder \\$ c0e9-4171-908e-08a611b84ff6}[icon]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765dc0e9-4171-908e-08a611b84ff6}[security]

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{2b0f765d-1644\} \\ folder \\ descriptions \setminus \{2b0f76d-1644\} \\ folder \\$ c0e9-4171-908e-08a611b84ff6}[streamresource]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765dc0e9-4171-908e-08a611b84ff6}[streamresourcetype]

c0e9-4171-908e-08a611b84ff6}[localredirectonly]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765dc0e9-4171-908e-08a611b84ff6}[roamable]

c0e9-4171-908e-08a611b84ff6}[precreate]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-16444, 2b0f765d-16444, 2b0f766d-16444, 2b0f76d-16444, 2b0f76d-16444$ c0e9-4171-908e-08a611b84ff6}[stream]

c0e9-4171-908e-08a611b84ff6}[publishexpandedpath]

c0e9-4171-908e-08a611b84ff6}[attributes]

Oueries value:

c0e9-4171-908e-08a611b84ff6}[foldertypeid]

Oueries value:

c0e9-4171-908e-08a611b84ff6}[initfolderhandler]

Oueries value:

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

folders[cookies]

Queries value:

65f9-4cf6-a03a-e3ef65729f3d}[category]

65f9-4cf6-a03a-e3ef65729f3d}[name]

Queries value:

65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]

65f9-4cf6-a03a-e3ef65729f3d}[description]

65f9-4cf6-a03a-e3ef65729f3d}[relativepath]

65f9-4cf6-a03a-e3ef65729f3d}[parsingname]

65f9-4cf6-a03a-e3ef65729f3d}[infotip]

65f9-4cf6-a03a-e3ef65729f3d}[localizedname]

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus current \\ version \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus current \\ version \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus current \\ version \setminus \{3eb685 \\ db-microsoft \setminus \{3eb685 \\ db-mic$ 65f9-4cf6-a03a-e3ef65729f3d}[icon]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[security]

65f9-4cf6-a03a-e3ef65729f3d}[streamresource]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype] Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ (3eb685db-10eb) \ description \ (3eb685db-10eb) \$ 65f9-4cf6-a03a-e3ef65729f3d}[roamable]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ between the constant \ folder \ between the constant \ folder \ fold$ 65f9-4cf6-a03a-e3ef65729f3d}[precreate]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[stream]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[attributes]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]

65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]

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

folders[appdata]

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]

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

settings\5.0\cache\history[peruseritem]

Queries value: $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet$

```
settings\5.0\cache\history[peruseritem]
  Queries value:
HKLM\software\wow6432node\microsoft\win
b784-432e-a781-5a1130a75963}[category]
```

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [name]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [parent folder]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [description]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [relative path]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [parsing name]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} [infotip]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} [icon]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ for the context of the context of$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [stream resource]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} [stream resource type]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [local redirectionly]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [roamable]$

Queries value:

Queries value:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [stream]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [publish expanded path]$

Queries value:

 $\label{thm:local-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \descriptions \folder \folder \descriptions \folder \f$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [folder typeid]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [initfolder \ handler]$

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

folders[history]

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

settings\5.0\cache\history[cachelimit]

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

settings\5.0\cache\extensible cache\domstore[cacherepair]

Queries 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]

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

settings\5.0\cache\extensible cache\domstore[cachelimit]

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

settings\5.0\cache\extensible cache\feedplat[cachepath]

Queries 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]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacherepair]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cachepath]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries 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]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\ietld[cacherepair]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries 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]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\ietld[cachelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\ietld[cacheoptions]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cacherepair]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cachepath]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\privacie:[cachelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
 Oueries value:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[displayscriptdownloadfailureui]
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[mbcsservername]
                           \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \notation{Internet}{ll} \end{tabular}
 Queries value:
settings[mbcsapiforcrack]
                           \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
 Oueries value:
settings[utf8servernameres]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
 Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablereadrange]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[socketsendbufferlength]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[keepalivetimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
 Queries value:
settings[maxconnectionsperserver]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1 Oserver]
 Queries value:
                           settings[maxconnectionsper1_0server]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperproxy]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[serverinfotimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[connecttimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
 Queries value:
                           HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
settings[connectretries]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendtimeout]
 Queries value:
                           HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
settings[sendtimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
```

```
settings[receivetimeout]
                                      HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
settings[receivetimeout]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
  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} in the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu
settings[scavengecachelowerbound]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[certcachenovalidate]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache[scavengecachefilelimit]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache[scavengecachefilelimit]
                                      HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache[scavengecachefilelimit]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[httpdefaultexpirytimesecs]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[ftpdefaultexpirytimesecs]
                                      HKLM\software\wow6432node\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[sim8c5.exe]
                                      HKLM\software\wow6432node\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
                                      \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
  Oueries value:
settings[disablecachingofsslpages]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[perusercookies]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[leashlegacycookies]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dialupuselansettings]
                                      HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings[dialupuselansettings]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[sendextracrlf]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasshttpnocachecheck]
  Queries value:
                                      HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
                                      HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasssslnocachecheck]
  Queries value:
                                      HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[enablehttptrace]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
                                      HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
settings[nocheckautodialoverride]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Queries value:
                                      HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
settings[dontusednsloadbalancing]
  Oueries value:
                                      HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[mimeexclusionlistforcache]
  Oueries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[dnscacheenabled]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[dnscacheentries]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dnscachetimeout]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonpost]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnalwaysonpost]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonbadcertrecving]
  Oueries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonhttpstohttpredirect]
```

Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings[tcpautotuning]

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

settings\wpad[wpadoverride]

HKLM\system\currentcontrolset\services\winsock\parameters[transports] Oueries value:

Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]

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

Oueries value: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip[winsock 2.0 provider id]

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname] HKCU\software\microsoft\windows\currentversion\internet Queries value:

settings[enableautodial]

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

settings[nonetautodial]

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

settings[globaluseroffline]

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

settings[badproxyexpirestime]

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet$ Queries value:

settings[disablebranchcache]

HKLM\software\wow6432node\microsoft\internet Oueries value:

explorer\main\featurecontrol\feature_http_username_password_disable[sim8c5.exe]

HKLM\software\wow6432node\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_http_username_password_disable[*]

 $HKLM \verb|\software| wow 6432 node \verb|\microsoft| tracing[enable consoletracing]|$ Queries value:

Queries value:

 $HKLM \setminus software \setminus wow 6432 node \setminus tracing \setminus sim8c5_rasapi32 [enable file tracing]$

HKLM\software\wow6432node\microsoft\tracing\sim8c5_rasapi32[filetracingmask]

Oueries value:

HKLM\software\wow6432node\microsoft\tracing\sim8c5_rasapi32[enableconsoletracing]

Queries value:

 $HKLM \verb|\software| wow 6432 node \verb|\microsoft| tracing \verb|\sim8c5_rasapi32[consoletracing mask]| \\$

 $HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus tracing \setminus sim8c5_rasapi32 [maxfilesize]$

Oueries value:

HKLM\software\wow6432node\microsoft\tracing\sim8c5_rasapi32[filedirectory]

HKLM\software\microsoft\windows Oueries value:

nt\currentversion\profilelist[programdata]

Oueries value: $HKLM \setminus software \setminus microsoft \setminus sqmclient \setminus windows \setminus disabled processes \texttt{[6aab869]}$

Queries value:

HKLM\software\microsoft\samclient\windows\disabledsessions[machinethrottling]

Queries value:

HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession] Oueries value:

HKLM\software\wow6432node\microsoft\tracing\sim8c5_rasmancs[enablefiletracing] Queries value:

HKLM\software\wow6432node\microsoft\tracing\sim8c5_rasmancs[filetracingmask]

Queries value:

HKLM\software\wow6432node\microsoft\tracing\sim8c5_rasmancs[enableconsoletracing]

Oueries value:

HKLM\software\wow6432node\microsoft\tracing\sim8c5_rasmancs[consoletracingmask]

HKLM\software\wow6432node\microsoft\tracing\sim8c5_rasmancs[maxfilesize]

Queries value:

HKLM\software\wow6432node\microsoft\tracing\sim8c5_rasmancs[filedirectory]

HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist] Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet Oueries value:

settings[proxysettingsperuser]

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

settings[migrateproxy]

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

settings[proxyenable]

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

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

settings\connections[savedlegacysettings]

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

settings\connections[defaultconnectionsettings]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1777f761-1616\} \ descriptions \$

68ad-4d8a-87bd-30b759fa33dd}[category]

Queries value:

```
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[parsingname]
```

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$

Queries value:

 $\label{lem:hkkm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\explorer\folderdescriptions\currentversion\explorer\explore$

Oueries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1777f761-68ad-4d8a-87bd-30b759fa33dd\} [security]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1777f761-68ad-4d8a-87bd-30b759fa33dd\} [stream resource]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1777f761-68ad-4d8a-87bd-30b759fa33dd\} [stream resource type]$

Queries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1777f761-68ad-4d8a-87bd-30b759fa33dd\} [local redirectonly]$

Queries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1777f761-68ad-4d8a-87bd-30b759fa33dd\} \ [roamable]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1777f761-68ad-4d8a-87bd-30b759fa33dd\}[precreate]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\eqnumber 1777f761-68ad-4d8a-87bd-30b759fa33dd\end{array} [stream]$

Queries value

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$

Queries value:

 $\label{lem:hamman} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\capable{lem:hamman} \{1777f761-68ad-4d8a-87bd-30b759fa33dd\}[attributes]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\eqnumber 1777f761-68ad-4d8a-87bd-30b759fa33dd\end{foldertypeid}$

Queries value:

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

folders[favorites]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags[{d97b6486-0cfa-44d8-acc2-0f8b5941e889}]

Queries value: HKCU\software\microsoft\windows

nt\currentversion\appcompatflags[{d97b6486-0cfa-44d8-acc2-0f8b5941e889}]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags[{44480e68-dfd5-435f-bdfe-b8246fc9f90f}]

Queries value: HKCU\software\microsoft\windows

nt\currentversion\appcompatflags[{44480e68-dfd5-435f-bdfe-b8246fc9f90f}]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[sim8c5.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet

Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature mime handling[*1

Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdl1]

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [prioritize record data]$

Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [direct access query order]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol] HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [register primary name]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount] Queries value: Queries value: Queries value: $\label{lem:hklm} \verb+Kklm \system \current control set \services \$ Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazv] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite] HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Queries value: 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] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [maxcached sockets]$ Queries value:

```
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [multicasts ender flags]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout]
  Oueries value:
                           HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
                           HKLM\software\wow6432node\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_unc_savedfilecheck[sim8c5.exe]
                           HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_unc_savedfilecheck[*]
                           HKLM\software\policies\microsoft\internet
  Oueries value:
explorer\security[disablesecuritysettingscheck]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\zones\0[flags]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\2[flags]
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings\zones\3[flags]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[flags]
                           HKCU\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[sim8c5.exe]
                           HKCU\software\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature localmachine lockdown[*]
  Queries value:
                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[sim8c5.exe]
                           HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
                           \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
  Oueries value:
settings[createuricachesize]
  Queries value:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[createuricachesize]
  Queries value:
                           settings[createuricachesize]
  Oueries value:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
 Queries value:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[enablepunvcode]
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
  Queries value:
settings\zonemap[autodetect]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\3[1a10]
  Queries value:
                           HKLM\system\currentcontrolset\control\wmi\security[5ef9ec44-fb87-4f51-
af4e-ced0840132811
  Queries value:
                           HKLM\system\currentcontrolset\control\wmi\security[7930f74b-e328-4350-
89c6-11fd93771488]
                           HKLM\software\microsoft\windows\windows error reporting[traceflags]
  Oueries value:
  Queries value:
                           HKLM\software\microsoft\windows\windows error reporting[noreflection]
  Queries value:
                           HKCU\software\microsoft\windows\windows error reporting[noreflection]
  Oueries value:
                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation[sim8c5.exe]
  Oueries value:
                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature zone elevation[*1
  Oueries value:
                           HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6[winsock 2.0 provider id]
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \{ parameters \setminus winsock [minsock addrlength] \}
```

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]

Oueries value:

 $\label{lem:hklm} \verb+kklm/system/currentcontrolset/services/tcpip6/parameters/winsock[usedelayedacceptance] \\$

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]

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

Oueries value:

Oueries value:

 $HKLM \ system \ current control set \ services \ tcpip6 \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [search list]$

Oueries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [enabled \ hcp]$

Oueries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [registration enabled]$

Queries value:

 $HKLM \system \current control set \services \true \parameters \true faces \end{22873b3e-c4d3-495a-8165-e1e01c1f69b5} \[register adapter name]$

Oueries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \tcpip \parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [domain]$

Queries value:

 $\label{lem:hklm} HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [dhcpdomain]$

Oueries value:

 $HKLM \ system \ current control set \ services \ tcpip6 \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [dhcpv6domain]$

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip6 \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [nameserver]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [names erver]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\}[dhcpnameserver]$

Queries value:

 $\label{thm:local-bound} $HKLM \simeq \sum_{i=1}^{100} \frac{446ee^342-7039-11de-9d^20-806e^66e^6963}{[enabledhcp]} $$ $HCM_{SYS}(0) = \frac{1}{2} \frac{$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '{846ee342-7039-11de-9d20-806e6f6e6963} \ [registration enabled]$

Queries value:

 $\label{lem:hklm} HKLM \system \current control set \services \tcpip \parameters \ interfaces \ \{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [register adapter name]$

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[domain]

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \tcpip \parameters \ interfaces \ \{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [dhcpdomain]$

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[nameserver]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpnameserver]

Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [queryadaptername]$

Queries value:

 $\label{lem:hklm} HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [disable adapter domain name]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [registration maxaddress count]$

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [maxnumber of addresses to register]$

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [enablemulticast]$

Queries value:

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '{846ee342-7039-11de-9d20-806e6f6e6963} \ [disable adapter domain name]$

Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[disabledynamicupdate] 806e6f6e6963}[enableadapterdomainnameregistration] HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registrationmaxaddresscount] $HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{846ee 342-7039-11de-9d20-11de-$ 806e6f6e6963}[maxnumberofaddressestoregister] Oueries value: 806e6f6e6963}[enablemulticast] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist] Queries value: HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension] Queries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity] Oueries value: HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder] Queries value: HKLM\system\currentcontrolset\services\ldap[usehostnameasalias] Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow] HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh] Oueries value: Queries value: HKCU\software\microsoft\internet explorer\ietld[ietldversionlow] Queries value: HKCU\software\microsoft\internet explorer\ietld[ietldversionhigh] $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}$ Queries value: settings\zones\3[{aeba21fa-782a-4a90-978d-b72164c80120}] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[privacyadvanced] Queries value: HKCU\software\microsoft\windows nt\currentversion\appcompatflags[showdebuginfo] HKLM\software\wow6432node\microsoft\windows Queries value: nt\currentversion\compatibility32[rundll32] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache[signature] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\lowcache\content[peruseritem] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\lowcache\content[cacheprefix] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\lowcache\content[cachelimit] HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\cookies[peruseritem] $\label{thm:linear} \verb+HKCU \software \microsoft \windows \current version \current \\$ Queries value: settings\5.0\lowcache\cookies[cacheprefix] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\lowcache\cookies[cachelimit] HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\history[peruseritem] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\history[cacheprefix] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\lowcache\history[cachelimit] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\lowcache\extensible cache\feedplat[cacherepair] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\feedplat[cachepath] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\lowcache\extensible cache\feedplat[cacheprefix] HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\feedplat[cachelimit] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\feedplat[cacheoptions] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\lowcache\extensible cache\iecompat[cacherepair] HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\iecompat[cachepath] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\iecompat[cacheprefix] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\lowcache\extensible cache\iecompat[cachelimit] HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\iecompat[cacheoptions] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\ietld[cacherepair] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\ietld[cachepath] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\ietld[cacheprefix] Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\lowcache\extensible cache\ietld[cachelimit]

settings\5.0\lowcache\extensible cache\ietld[cacheoptions]

Oueries value:

HKCU\software\microsoft\windows\currentversion\internet

```
Oueries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\privacie:[cacherepair]
  Oueries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\privacie:[cachepath]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\lowcache\extensible cache\privacie:[cacheprefix]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\privacie:[cachelimit]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\privacie:[cacheoptions]
                                     HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[rundll32.exe]
                                      HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a66e19e6]
  Queries value:
  Sets/Creates value:
                                     HKLM\system\currentcontrolset\control\session
manager[pendingfilerenameoperations]
  Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\run[1h6wzb8fyvuwzwwulyaty]
  Sets/Creates value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1409]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Sets/Creates value:
settings\zones\0[1609]
  Sets/Creates value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1406]
  Sets/Creates value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1[1406]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Sets/Creates value:
settings\lockdown_zones\2[1406]
  Sets/Creates value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3[1406]
  Sets/Creates value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4[1406]
                                     HKCU\software\microsoft\internet
  Sets/Creates value:
explorer\phishingfilter[shownservicedownballoon]
  Sets/Creates value:
                                     HKCU\software\microsoft\internet
explorer\recovery[clearbrowsinghistoryonexit]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Sets/Creates value:
settings[globaluseroffline]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\sim8c5_rasapi32[enablefiletracing]
  Sets/Creates value:
HKLM \verb|\software| wow 6432 node \verb|\microsoft| tracing \verb|\sim8c5_rasapi32[enable consoletracing]| \\
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\sim8c5_rasapi32[filetracingmask]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\sim8c5_rasapi32[consoletracingmask]
                                     HKLM\software\wow6432node\microsoft\tracing\sim8c5_rasapi32[maxfilesize]
  Sets/Creates value:
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\sim8c5_rasapi32[filedirectory]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\sim8c5_rasmancs[enablefiletracing]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\sim8c5_rasmancs[enableconsoletracing]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\sim8c5_rasmancs[filetracingmask]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\sim8c5_rasmancs[consoletracingmask]
  Sets/Creates value:
                                      HKLM\software\wow6432node\microsoft\tracing\sim8c5_rasmancs[maxfilesize]
  Sets/Creates value:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus sim8c5\_rasmancs[filedirectory]
                                      HKCU\software\microsoft windows[00000028538b6f3a]
  Sets/Creates value:
  Value changes:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Value changes:
settings[proxyhttp1.1]
  Value changes:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Value changes:
settings[warnonpostredirect]
  Value changes:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[warnonintranet]
  Value changes:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1409]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Value changes:
settings\zones\1[1609]
  Value changes:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1406]
  Value changes:
                                      \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings\zones\2[1409]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Value changes:
settings\zones\2[1609]
  Value changes:
                                      \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} in the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu
settings\zones\2[1406]
  Value changes:
                                      HKCU\software\microsoft\windows\currentversion\internet
```

settings\zones\3[1409] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1609] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1406] Value changes: $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}$ settings\zones\4[1409] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\zones\4[1609] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[1406] $\label{thm:local_equation} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\phishingfilter[enabledv8]}}$ Value changes: Value changes: $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ settings[proxyenable] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\connections[savedlegacysettings] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[uncasintranet] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[autodetect]

Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[globaluseroffline]