# Malware Analysis Appliance by Blue Coat Systems, Inc.

#### Task Details

Host: mag2, Sample ID: 5011, Task ID: 40062

Task ID: 40062 Risk Level: 10

Date Processed: 2016-05-03 05:04:46 (UTC)

Processing Time: 62.08 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\spyeye\_injector.exe"

Sample ID: 5011
Type: basic
Owner: admin

Label: spyeye\_injector.exe
Date Added: 2016-05-03 05:04:45 (UTC)

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

MD5: b98bb6d7428c3dbffcfcab2414c6daa2

SHA256: fc7f54ce456c164452d8429a7fd5f52629a69338f8954e287d2664c03c37e029

Description: None

### Pattern Matching Results

- 10 Suspicious writeprocess: Spyeye [Banking]
- 10 Creates malicious mutex: Spyeye [Banking]
- 2 PE: Nonstandard section
- 6 Renames file on boot
- 4 Terminates process under Windows subfolder
- 6 Notifies system about Internet connection change
- 6 Modifies registry autorun entries
- 1 HTTP connection response code 404 (file not found)
- Writes to memory of system processes
- 5 Packer: UPX
- 3 Program causes a crash [Info]
- 5 Adds autostart object
- 4 Reads process memory
- 3 HTTP connection response code 200 (success)
- 5 Abnormal sleep detected
- 5 PE: Contains compressed section

#### Static Events

Reads from process:

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\CGU1EED.exe

["C:\Users\Admin\AppData\Local\Temp\CGU1EED.exe"]

Creates process: C:\Windows\SysWOW64\rundll32.exe ["C:\Windows\system32\rundll32.exe"

PID:348 C:\Windows\System32\wininit.exe

"C:\Windows\syswow64\WININET.dll",DispatchAPICall 1 ]
Reads from process: PID:340 C:\Windows\explorer.exe

PID:400 C:\Windows\System32\winlogon.exe Reads from process: Reads from process: PID:444 C:\Windows\System32\lsass.exe Reads from process: PID:452 C:\Windows\System32\lsm.exe PID:568 C:\Windows\System32\svchost.exe Reads from process: Reads from process: PID:636 C:\Windows\System32\svchost.exe Reads from process: PID:688 C:\Windows\System32\svchost.exe PID:796 C:\Windows\System32\svchost.exe Reads from process: Reads from process: PID:848 C:\Windows\System32\svchost.exe Reads from process: PID:952 C:\Windows\System32\svchost.exe Reads from process: PID:844 C:\Windows\System32\dwm.exe Reads from process: PID:1068 C:\Windows\System32\spoolsv.exe Reads from process:

Reads from process: PID:1100 C:\Windows\System32\spootsvexe PID:1100 C:\Windows\System32\svchost.exe Reads from process: PID:1120 C:\Windows\System32\svchost.exe PID:1188 C:\Windows\System32\svchost.exe Reads from process: PID:1396 C:\Windows\System32\svchost.exe PID:1804 C:\Windows\System32\svchost.exe PID:1804 C:\Windows\System32\svchost.exe PID:1804 C:\Windows\System32\svchost.exe PID:1804 C:\Windows\System32\svchost.exe PID:1804 C:\Windows\System32\svchost.exe

Reads from process: PID:272 C:\Windows\System32\taskhost.exe
Reads from process: PID:1552 C:\Windows\System32\taskhost.exe
Reads from process: PID:364 C:\Windows\System32\taskhost.exe
Reads from process: PID:808 C:\Windows\System32\tonhost.exe
Reads from process: PID:2112 C:\Windows\System32\mobsync.exe
Reads from process: PID:2660 C:\Windows\System32\mobsync.exe

Reads from process: PID:2764 C:\Windows\System32\wbem\WmiPrvSE.exe Reads from process: PID:2824 C:\Windows\System32\conhost.exe

D	DTD-4644 CANCAL
Reads from process:	PID:1644 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:1300 C:\Program Files (x86)\Adobe\Reader 9.0\Reader\reader_sl.exe
Writes to process:	PID:2916 C:\Users\Admin\AppData\Local\Temp\CGU1EED.exe
Writes to process:	PID:3036 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:1644 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2072 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:344 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2200 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2184 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2240 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2296 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2284 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2316 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2336 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2308 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2340 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2360 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2332 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2364 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2356 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2388 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2408 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2380 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2412 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2432 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2512 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2500 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2580 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2596 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2600 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2588 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2828 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2832 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2852 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:1548 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2748 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2864 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:500 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:656 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:972 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2704 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2744 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2732 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2692 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2220 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:1668 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2212 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2928 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:1860 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:1152 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:1948 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:1712 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2252 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:248 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2236 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:1740 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2420 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:1628 C:\Windows\SysWOW64\rundll32.exe
Terminates process:	C:\WinOldFileq\83A49421CBD.exe
Terminates process:	C:\Windows\Temp\spyeye_injector.exe
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 00000000
Creates mutex:	\BaseNamedObjects\EGg7ES3EmkOecYoUeMUM9KK13GQy9WS
Creates mutex:	\Sessions\1\BaseNamedObjects\_!MSFTHISTORY!_
Creates mutex:	

 $\label{local:microsoft:windows:temporary internet} $$ \operatorname{local:microsoft:windows:temporary internet files:content.ie5!} $$$ 

Creates mutex:

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

Creates mutex: \Sessions\1\BaseNamedObjects\WininetStartupMutex
Creates mutex: \Sessions\1\BaseNamedObjects\WininetConnectionMutex
Creates mutex: \Sessions\1\BaseNamedObjects\WininetProxyRegistryMutex

Creates mutex: \Sessions\1\BaseNamedObjects\RasPbFile

Creates mutex: \Sessions\1\BaseNamedObjects\ZonesCounterMutex

Creates mutex: \Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex
Creates mutex: \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex

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 mutex: \Sessions\1\BaseNamedObjects\!IETld!Mutex
Creates event: \BaseNamedObjects\SvcctrlStartEvent\_A3752DX
Creates event: \Security\LSA\_AUTHENTICATION\_INITIALIZED
Creates event: \KernelObjects\SystemErrorPortReady

Creates event: \BaseNamedObjects\BFE\_Notify\_Event\_{a60085e8-950a-439c-a424-

c0d15d0a30bd}

Creates semaphore: \Sessions\1\BaseNamedObjects\4FBEA4B1

### File System Events

Creates: C:\WinOldFileq
Creates: C:\WinOldFileq\

Creates: C:\WinOldFileq\83A49421CBD.exe
Creates: C:\WinOldFileq\8FDC7C717274206
Creates: C:\Users\Admin\AppData\Local\Temp\

Creates: C:\Users\Admin\AppData\Local\Temp\CGU1EED.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\CGU1EED.exe

Creates: C:\Users\Admin

Creates: C:\Users\Admin\AppData\Local

Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files

Creates: C:\Users\Admin\AppData\Roaming

Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\History

Creates: C:\Users\Admin\Favorites

Opens: C:\Windows\Prefetch\SPYEYE\_INJECTOR.EXE-619282B0.pf

Opens: C:\Windows

 Opens:
 C:\Windows\System32\wow64.dl1

 Opens:
 C:\Windows\System32\wow64win.dl1

 Opens:
 C:\Windows\System32\wow64cpu.dl1

 Opens:
 C:\Windows\system32\wow64log.dl1

Opens: C:\Windows\SysWOW64

Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\Windows\SysWOW64\kernel32.dll

Opens: C:\

 ${\tt Opens:} \hspace{1.5cm} {\tt C:\Windows\backslash Globalization\backslash Sorting\backslash SortDefault.nls} \\$ 

Opens: C:\Windows\SysWOW64\ntdll.dll

Opens: C:\WinOldFileq
Opens: C:\WinOldFileq\

Opens: C:\Windows\Temp\spyeye\_injector.exe
Opens: C:\WinOldFileq\83A49421CBD.exe
Opens: C:\Windows\SysWOW64\apphelp.dll
Opens: C:\Windows\AppPatch\sysmain.sdb
Opens: C:\WinOldFileq\ui\SwDRM.dll

Opens: C:\Windows\Prefetch\83A49421CBD.EXE-8B5C1E36.pf

 Opens:
 C:\Windows\SysWOW64\imm32.dl1

 Opens:
 C:\Win0ldFileq\MSIMG32.dl1

 Opens:
 C:\Windows\SysWOW64\msimg32.dl1

 Opens:
 C:\Win0ldFileq\8FDC7C717274206

 Opens:
 C:\Users\Admin\AppData\Local\Temp

Opens: C:\Users\Admin\AppData\Local\Temp\CGU1EED.exe

Opens: C:\Users
Opens: C:\Users\Admin
Opens: C:\Users\Admin\AppData

Opens: C:\Users\Admin\AppData\Local

Opens: C:\Users\Admin\AppData\Local\Temp\ui\SwDRM.dll
Opens: C:\Windows\Prefetch\CGU1EED.EXE-9423C11C.pf
Opens: C:\Users\Admin\AppData\Local\Temp\MSIMG32.dll

Opens: C:\windows\temp\spyeye\_injector.exe

Opens: C:\Program Files (x86)\Adobe\Reader 9.0\Reader\MSIMG32.dll

Opens: C:\Windows\SysWOW64\wininet.dll

Opens: C:\Users\Admin\AppData\Local\Temp\USERENV.dll

Opens: C:\Windows\SysWOW64\userenv.dll

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

 $\label{lem:continuous} Opens: $$C:\Users\land \naming\Microsoft\SystemCertificates\My\CRLs$$ Opens: $$C:\Users\land \naming\Microsoft\SystemCertificates\My\CTLs$$$ 

 Opens:
 C:\Windows\SysWOW64\user32.dl1

 Opens:
 C:\Windows\SysWOW64\ws2\_32.dl1

```
C:\Windows\SysWOW64\advapi32.dll
  Opens:
                                     C:\Windows\SysWOW64\crypt32.dll
  Opens:
  Opens:
                                     C:\Windows\SysWOW64\tzres.dll
                                     C:\Windows\SysWOW64\en-US\tzres.dll.mui
  Opens:
  Opens:
                                     C:\Users\Admin\AppData\Local\Temp\CGU1EED.exe.Local\
  Opens:
                                     C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
                                     C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
  Opens:
                                     C:\Windows\WindowsShell.Manifest
                                     C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
  Opens:
  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
  Opens:
                                     C:\Users\Admin\AppData\Roaming
  Opens:
                                     C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
                                     C:\Users\Admin\AppData\Local\Microsoft\Windows\History
  Opens:
  Opens:
                                     C:\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
  Opens:
                                     C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\index.dat
  Opens:
                                     C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
  Opens:
\label{lem:c:start} C: \label{lem:c:start} Admin\ App Data \ Local\ Microsoft\ Windows\ History\ . IE5\ index.\ data \ 
  Opens:
                                     C:\Windows\SysWOW64\mswsock.dll
  Opens:
                                     C:\Windows\SysWOW64\WSHTCPIP.DLL
  Opens:
                                     C:\Users\Admin\AppData\Local\Temp\dnsapi.DLL
  Opens:
                                     C:\Windows\SysWOW64\dnsapi.dll
  Opens:
                                     C:\Users\Admin\AppData\Local\Temp\iphlpapi.DLL
  Opens:
                                     C:\Windows\SysWOW64\IPHLPAPI.DLL
  Opens:
                                     C:\Users\Admin\AppData\Local\Temp\WINNSI.DLL
  Opens:
                                     C:\Windows\SysWOW64\winnsi.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
  Opens:
                                     C:\Windows\SysWOW64\rtutils.dll
                                     C:\ProgramData\Microsoft\Network\Connections\Pbk\
  Opens:
  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
                                     C:\Users\Admin\AppData\Local\Microsoft\Windows
  Opens:
                                     C:\Users\Admin\AppData\Local\Microsoft
  Opens:
  Opens:
                                     C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\Low
                                     C:\Users\Admin\AppData\Roaming\Microsoft\Windows
  Opens:
  Opens:
                                     C:\Users\Admin\AppData\Roaming\Microsoft
  Opens:
                                     C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low
  Opens:
                                     C:\Users\Admin\Favorites
  Opens:
                                     C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Virtualized
  Opens:
                                     C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE
  Opens:
                                     C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE\Low
                                     Opens:
  Opens:
                                     C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache\Low
  Opens:
                                     C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache
  Opens:
                                     C: \verb|\USers\Admin\AppData\Roaming\Microsoft\Windows\IETldCache\Low|
  Opens:
                                     C:\Users\Admin\AppData\Local\Temp\Low
  Opens:
                                     C:\Windows\SysWOW64\rundll32.exe
                                     C:\Windows\SysWOW64\ui\SwDRM.dll
  Opens:
  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\Prefetch\WERFAULT.EXE-37549B7E.pf
  Opens:
                                     C:\Windows\SysWOW64\psapi.dll
  Opens:
                                     C:\Windows\AppPatch\AcLayers.dll
                                     C:\Windows\SysWOW64\winspool.drv
  Opens:
  Opens:
                                     C:\Windows\SysWOW64\mpr.dll
  Opens:
                                     C:\Windows\AppPatch\acwow64.dll
  Opens:
                                     C:\Windows\SysWOW64\version.dll
  Opens:
                                     C:\Windows\SysWOW64\en-US\rundll32.exe.mui
  Opens:
                                     C:\Windows\syswow64\WININET.dll.manifest
                                     C:\Windows\SysWOW64\uxtheme.dll
  Opens:
```

C:\Windows\SysWOW64\dwmapi.dll

Opens:

C:\Windows\SysWOW64\rundl132.exe.Local\ Opens:

C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Opens:

Files\Low\desktop.ini

Opens: Files\Low\Content.IE5 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

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

Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Low\Content.IE5\index.dat

 $C: \verb|\USers\Admin\AppData\Roaming\Microsoft\Windows\Cookies\Low\Index.dat|$ Opens:

Opens:

C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\History.IE5\index.dat

Opens: C:\Windows\SvsWOW64\NapiNSP.dll Opens: C:\Windows\SysWOW64\pnrpnsp.dll Opens: C:\Windows\SysWOW64\winrnr.dll

C:\Users\Admin\AppData\Local\Temp\dhcpcsvc6.DLL Opens:

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:\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\en-US\urlmon.dll.mui

C:\Windows\SysWOW64\wship6.dll Opens: Opens: C:\Windows\SysWOW64\FWPUCLNT.DLL Writes to: C:\WinOldFileq\83A49421CBD.exe Writes to: C:\WinOldFileq\8FDC7C717274206

Writes to: C:\Users\Admin\AppData\Local\Temp\CGU1EED.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:\WinOldFileq\8FDC7C717274206

 ${\tt C:\Users\Admin\AppData\Local\Temp\CGU1EED.exe}$ Reads from:

Reads from: C:\Windows\SysWOW64\user32.dll 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\rundl132.exe Reads from: C:\Windows\System32\drivers\etc\hosts C:\Windows\Temp\spyeye\_injector.exe Deletes:

#### Network Events

DNS query: alexeyartemov.com DNS query: www.microsoft.com

DNS response: alexeyartemov.com ⇒ 198.105.244.11 alexeyartemov.com ⇒ 104.239.213.7 DNS response: DNS response: e10088.dspb.akamaiedge.net  $\Rightarrow$  96.6.72.154 DNS response: e10088.dspb.akamaiedge.net ⇒ 104.109.84.116

Connects to: 88.198.13.147:443 Connects to: 8.8.8.8:53 Connects to: 4.2.2.1:53 Connects to: 198.105.244.11:80 Connects to: 104.239.213.7:80 96.6.72.154:80 Connects to: Sends data to: 8.8.8.8:53 Sends data to: 4.2.2.1:53 Sends data to: 88.198.13.147:443

Sends data to: alexeyartemov.com:80 (198.105.244.11) Sends data to: alexeyartemov.com:80 (104.239.213.7) Sends data to: e10088.dspb.akamaiedge.net:80 (96.6.72.154)

Receives data from: 8.8.8.8:53 Receives data from: 4.2.2.1:53 Receives data from: 88.198.13.147:443

Receives data from: alexeyartemov.com:80 (198.105.244.11) Receives data from: alexeyartemov.com:80 (104.239.213.7) Receives data from: e10088.dspb.akamaiedge.net:80 (96.6.72.154)

## Windows Registry Events

HKLM\system\currentcontrolset\control\session manager
<pre>HKCU\software\microsoft\windows\currentversion\run</pre>
<pre>HKCU\software\microsoft\windows\currentversion\internet settings</pre>
<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\0</pre>
HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\2</pre>
<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\3</pre>
<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\4</pre>

```
HKCU\software\microsoft\windows\currentversion\internet
 Creates key:
settings\lockdown_zones\1
                          HKCU\software\microsoft\windows\currentversion\internet
 Creates key:
settings\lockdown_zones\2
 Creates kev:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                          HKCU\software\microsoft\windows\currentversion\internet
 Creates key:
settings\lockdown_zones\4
 Creates key:
                          HKCU\software\microsoft\internet explorer\phishingfilter
                          HKCU\software\microsoft\internet explorer\recovery
 Creates key:
 Creates key:
                          HKCU\software\microsoft\systemcertificates\my
 Creates key:
                          HKCU\software\microsoft windows
 Creates key:
                          HKLM\software\wow6432node\microsoft\tracing
                          HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32
 Creates key:
 Creates key:
                          HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasmancs
 Creates key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\connections
 Creates key:
                          HKCU\software\appdatalow
 Creates key:
                          HKCU\software\microsoft\internet explorer\internetregistry
                          HKCU\software\microsoft\internet explorer\lowregistry
 Creates key:
 Creates key:
                          HKCU\software\microsoft\internet
explorer\lowregistry\dontshowmethisdialogagain
 Creates kev:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache
 Creates key:
                          HKCU\software\microsoft\internet explorer\intelliforms
 Creates key:
                          HKCU\software\microsoft\internet explorer\toolbar
 Creates key:
                          HKCU\software\microsoft\internet explorer\toolbar\webbrowser
 Creates key:
HKCU\software\microsoft\windows\currentversion\explorer\menuorder\favorites
 Creates key:
                          HKCU\software\microsoft\internet explorer\pagesetup
 Creates key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\passport\lowdamap
 Creates key:
 Creates key:
 Creates key:
                          HKCU\software\microsoft\internet explorer\zoom
```

HKCU\software\microsoft\windows\currentversion\internet settings\wpad HKCU\software\microsoft\windows\currentversion\explorer\lowregistry

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

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

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

awareness

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

HKLM\software\wow6432node Creates key:

Creates key: HKLM\software\wow6432node\microsoft

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

settings\p3p\history

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

settings[proxyserver] Deletes value:

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

Deletes value:

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

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

settings\zonemap[proxybypass]  $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet$ 

Deletes value:

settings\zonemap[proxybypass] HKCU\software\microsoft\windows\currentversion\internet

Deletes value:

settings\zonemap[intranetname]

Deletes value:

 $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version\\| internet$ 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\wow6432node\policies\microsoft\windows\safer\codeidentifiers

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

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

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

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

Opens key: HKCU\

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

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

HKCU\control panel\desktop Opens key:

Opens key: HKCU\control panel\desktop\muicached

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

Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions

HKLM\ Opens key:

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

nt\currentversion\diagnostics

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

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

Opens key: HKLM\svstem\setup

Opens key: HKLM\svstem\currentcontrolset\control\nls\extendedlocale

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

options\83a49421cbd.exe

HKLM\system\currentcontrolset\control\session manager\appcertdlls Opens key: Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility HKLM\software\wow6432node\policies\microsoft\windows\appcompat Opens key:

HKLM\software\policies\microsoft\windows\appcompat Opens kev: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers Opens key:  $\label{local-operator} \mbox{HKCU\software\mbox{\sc microsoft\windows} nt\current\version\app\compatflags\layers} \\$ 

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\83a49421cbd.exe

Opens kev: HKLM\svstem\currentcontrolset\services\crvpt32

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

execution options\83a49421cbd.exe

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

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

nt\currentversion\appcompatflags\custom\83a49421cbd.exe

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

nt\currentversion\gre\_initialize

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

nt\currentversion\compatibility32

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

compatibility

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

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

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

settings Opens key:

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

settings

agent

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

options\cgu1eed.exe

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\cgu1eed.exe

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

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

Opens kev:

HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\user agent

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

settings\5.0\user agent

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet$ Opens key:

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

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

settings\user agent

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

Opens key:

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

settings\user agent Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet$ settings\user agent\ua tokens

Opens kev:

HKCU\software\microsoft\windows\currentversion\internet settings Opens key: settings\user agent\pre platform

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

settings\5.0\user agent\pre platform

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

settings\5.0\user agent\pre platform

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

settings\user agent\post platform

Opens key:

settings\5.0\user agent\post platform

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

settings\5.0\user agent\post platform

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

explorer\main\featurecontrol

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

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

explorer\main\featurecontrol

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

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_browser\_emulation

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

explorer\main\featurecontrol\feature\_browser\_emulation

Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid

Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 0
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype

0\certdllopenstoreprov

Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype

 ${\tt 0\certdllopenstoreprov\#16}$ 

Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype

0\certdllopenstoreprov\ldap

Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 1
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype

1\certdllopenstoreprov

Opens key: HKU\

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

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

 $nt \verb|\currentversion| profile list \verb|\s-1-5-21-980053277-1733835069-2361817685-1001| \\$ 

980053277-1733835069-2361817685-1001

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

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

Opens key: HKCU\software\microsoft\systemcertificates\my\crls
Opens key: HKCU\software\microsoft\systemcertificates\my\ctls
Opens key: HKCU\software\microsoft\systemcertificates\my\keys
Opens key: HKLM\system\currentcontrolset\control\cmf\config

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

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots

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

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

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

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

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

Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc

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

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

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

settings\5.0\cache

Opens key:  $\label{thm:consoftware} \mbox{HKCU\software\mbox{\mbox{microsoft\windows\currentversion\internet}}}$ 

settings\5.0\cache

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

settings\5.0\cache\content

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

settings\5.0\cache\content

Opens key:

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ f9d\}$ 

Opens key:

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

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

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in folders$ 

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

folders

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:

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

Opens key

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ ff 1b32785-6fba-4fcf-9d55-7b8e7f157091 \ property bag$ 

Opens key:

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

```
Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-microsoft \ windows \ node \ microsoft \ and \ node \ node
0e22-4760-9afe-ea3317b67173}\propertybag
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings
        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\cache\cookies
                                                                                                              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
      Opens kev:
 settings\5.0\cache\cookies
        Opens key:
c0e9-4171-908e-08a611b84ff6}
       Opens key:
```

c0e9-4171-908e-08a611b84ff6}\propertybag

Opens key: 65f9-4cf6-a03a-e3ef65729f3d}

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ folde$ 65f9-4cf6-a03a-e3ef65729f3d}\propertybag

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

settings\5.0\cache\history

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

settings\5.0\cache\history

Opens key:

b784-432e-a781-5a1130a75963}

Opens kev:

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

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

settings\5.0\cache\extensible cache

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

settings\5.0\cache\extensible cache\domstore

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

settings\5.0\cache\extensible cache\feedplat

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

settings\5.0\cache\extensible cache\iecompat

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

settings\5.0\cache\extensible cache\ietld

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

settings\5.0\cache\extensible cache\privacie:

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\retry\_headeronlypost\_onconnectionreset HKLM\software\wow6432node\microsoft\internet Opens key:  $\verb|explorer| \verb|main| feature control| retry_header on ly post\_on connection reset|$ Opens key:

HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_bufferbreaking\_818408

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

explorer\main\featurecontrol\feature\_bufferbreaking\_818408

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature\_skip\_post\_retry\_on\_internetwritefile\_kb895954

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

explorer\main\featurecontrol\feature\_skip\_post\_retry\_on\_internetwritefile\_kb895954

Opens key:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \$ 

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

settings\5.0\cache

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

settings\5.0\cache

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_fix\_chunked\_proxy\_script\_download\_kb843289

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

explorer\main\featurecontrol\feature\_fix\_chunked\_proxy\_script\_download\_kb843289

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_use\_cname\_for\_spn\_kb911149 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_use\_cname\_for\_spn\_kb911149

HKCU\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature\_disable\_notify\_unverified\_spn\_kb2385266 HKLM\software\wow6432node\microsoft\internet Opens kev:

explorer\main\featurecontrol\feature\_disable\_notify\_unverified\_spn\_kb2385266

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_compat\_use\_connection\_based\_negotiate\_auth\_kb2151543

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

explorer\main\featurecontrol\feature\_compat\_use\_connection\_based\_negotiate\_auth\_kb2151543

HKCU\software\microsoft\internet Opens kev:

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

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

```
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\17506cf5
 Opens kev:
                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
                    HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens key:
                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens key:
                    HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
 Opens 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
                    HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
                    HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                    HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
                    HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
                    HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens key:
Opens kev:
Opens kev:
Opens key:
HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens kev:
Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
 Opens kev:
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\00000000001
                    HKCU\software\microsoft\internet
 Opens key:
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
 Opens key:
Opens key:
                    HKCU\software\microsoft\internet
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:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\1b6e5dd2
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
 Opens key:
```

 $\label{lem:hklm} \verb+Kklm \system \current control set \services \swinsock \space{2mm} parameters$ 

Opens key:

```
Opens key:
                         HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
 Opens key:
                         HKLM\svstem\currentcontrolset\services\tcpip\parameters\winsock
 Opens kev:
                         HKLM\system\currentcontrolset\services\winsock\setup migration\providers
 Opens key:
                         HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
 Opens key:
                         \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\wpad}} \\
                         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
                         HKCU\software\microsoft\internet
 Opens kev:
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\cgu1eed_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:
 Opens key:
                         HKLM\system\currentcontrolset\control\sqmservicelist
 Opens key:
```

 $\label{thm:local-state} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \cal{local-state} \{1777f761-68ad-4d8a-87bd-30b759fa33dd\}$ 

Opens key:

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

options\rundll32.exe

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\rundl132.exe

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

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

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

explorer\main\featurecontrol\feature\_mime\_handling

Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient

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

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

nt\dnsclient\dnspolicyconfig

Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig

Opens key:

 ${\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ dns cache \verb|\ parameters \verb|\ dns policy config$ 

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

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

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

Opens key:

 $HKLM \verb|\software| wow 6432 node \verb|\policies| microsoft| windows \verb|\currentversion| internet| and the software \verb|\currentversion| internet and the software and the software \verb|\currentversion| internet and the software and the s$ 

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 kev:

 $HKLM \label{lem:hkkm} \label{lem:hkkm} HKLM \label{lem:hkkm} If the lem is a substitution of the lem$ 

settings\zonemap\ranges\

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

settings\zonemap\ranges

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

settings\zonemap\ranges\

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_unc\_savedfilecheck

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

explorer\main\featurecontrol\feature\_unc\_savedfilecheck

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

settings\zonemap\

Opens key: HKCU\software\microsoft\internet

Opens key:

 $\label{lem:hklmsoftwarewow6432node} HKLM\software\policies\microsoft\windows\currentversion\nternet$  Opens key:  $\mbox{HKLM\software\policies\microsoft\windows\currentversion\nternet}$ 

```
settings\zonemap
                                                   HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\zonemap
   Opens key:
                                                   HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
   Opens key:
                                                   HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\protocoldefaults\
   Opens key:
                                                   HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
   Opens key:
                                                   HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap\domains\
   Opens key:
                                                   HKLM\software\policies\microsoft\internet explorer\security
   Opens key:
                                                   HKCU\software\microsoft\windows\currentversion\internet settings\zones\
                                                   \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\zones\endown} \mbox{\tt 2} \mbox{\tt ones\scale} \mbox{\tt 0} \mbox{\tt ones\scale} \mbox{\tt on
   Opens key:
   Opens key:
                                                   HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
   Opens key:
                                                   HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
                                                   HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
   Opens kev:
   Opens key:
                                                   HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
   Opens key:
HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ current version \ internet settings \ zones \ \ windows \ constant \ description \ desc
   Opens key:
                                                   HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones
                                                   HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\zones\
   Opens key:
HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ current version \ internet\ settings \ vones \ \ 0
                                                   HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\zones\0
                                                   HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\zones\0
   Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\1
                                                   HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\zones\1
                                                   HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\zones\1
                                                   HKLM\software\wow6432node\microsoft\windows\currentversion\internet
   Opens kev:
settings\zonemap\
   Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\2
   Opens key:
                                                   HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
   Opens kev:
                                                   HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
   Opens kev:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\3
   Opens key:
                                                   \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\zones\3
                                                   HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
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 key:
settings\zones\4
   Opens key:
                                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature localmachine lockdown
   Opens key:
                                                   HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
   Opens key:
HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| windows\\| current version\\| internet
settings\lockdown_zones\
   Opens kev:
                                                   HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones
   Opens key:
                                                   HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                                                   HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\
                                                   HKCU\software\microsoft\windows\currentversion\internet
   Opens kev:
settings\lockdown_zones\0
   Opens kev:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
   Opens key:
                                                   \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\0
   Opens key:
                                                   HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Opens kev:
settings\lockdown_zones\1
   Opens key:
settings\lockdown_zones\1
```

```
Opens key:
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
  Opens key:
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\2
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
  Opens key:
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
  Opens key:
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\3
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown zones\3
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\4
  Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\lockdown_zones\4
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\4
  Opens key:
                                     HKLM\software\wow6432node\microsoft\windows nt\currentversion\aedebug
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\4
                                     HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
                                     HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
                                     HKLM\system\currentcontrolset\control\networkprovider\hworder
  Opens kev:
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\lowcache\content
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
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 key:
settings\5.0\lowcache\extensible cache
                                     \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{$microsoft$} \windows \current version \end{tabular} internet \\ \end{tabular}
  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 kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\00f5af79
                                     \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Opens key:
settings\connections
  Opens key:
                                     HKLM\software\wow6432node\policies\microsoft\system\dnsclient
  Opens key:
                                     HKLM\software\policies\microsoft\system\dnsclient
  Opens kev:
                                     HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache
  Opens key:
e1e01c1f69b5}
  Opens key:
                                     \label{lem:hklm} \verb+Kklm \system \current control set \services \tcpip \parameters \time faces
  Opens key:
e1e01c1f69b5}
  Opens kev:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}
  Opens key:
HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{846ee 342-7039-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-
806e6f6e6963}
  Opens kev:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a91d0a5e-390e-4979-9c38-
127795cce47a}
  Opens key:
65fee5bae0b1}
```

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_use\_ietldlist\_for\_domain\_determination

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

explorer\main\featurecontrol\feature\_use\_ietldlist\_for\_domain\_determination

Opens key: HKLM\system\currentcontrolset\control\lsa\accessproviders

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

migration\providers\tcpip6

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_zone\_elevation

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

explorer\main\featurecontrol\feature\_zone\_elevation

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

settings\p3p\history\microsoft.com

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

options[disableusermodecallbackfilter]

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

manager[cwdillegalindllsearch]

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

Queries value:

Queries value:

 $HKLM \verb|\system| current control \verb|\nls| language[install language fall back]|$ 

Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]

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

us[alternatecodepage]

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

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

Queries value:

 $HKLM \verb|\software| wow 6432 node \verb|\microsoft| windows \verb|\currentversion| side by side[prefer external manifest]| and the side of the sid$ 

 $\label{thm:current} Queries \ value: \\ HKLM \ system \ current controls et \ control \ nls \ sorting \ versions \ []$ 

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

Queries value:

HKLM\system\currentcontrolset\control\computername\activecomputername[computername]

Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup[systemsetupinprogress]

Queries value: HKLM\system\currentcontrol\scustomlocale[en-us] Queries value: HKLM\system\currentcontrol\set\control\nls\extendedlocale[en-us]

Queries value:

folders[cache]

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

options[disablelocaloverride]

Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]

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

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

nt\currentversion\compatibility32[83a49421cbd]

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

nt\currentversion\windows[loadappinit\_dlls]

Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings[disableimprovedzonecheck]

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

settings[security\_hklm\_only]

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

manager[pendingfilerenameoperations2]

 $\label{thm:current} Queries \ value: \\ HKLM\system\currentcontrolset\control\session$ 

manager[pendingfilerenameoperations]

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

nt\currentversion\compatibility32[cgu1eed]

Queries value: HKLM\software\wow6432node\microsoft\internet explorer[version] Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\user agent[]

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

settings\5.0\user agent[]

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

settings\5.0\user agent[compatible]

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

settings\5.0\user agent[compatible]

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

settings\5.0\user agent[version]

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

settings\5.0\user agent[version]

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

agent]

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

```
settings\5.0\user agent[platform]
                                   HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\user agent[platform]
  Queries value:
                                   HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation[cgu1eed.exe]
  Queries value:
                                   HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation[*]
                                   HKLM\system\currentcontrolset\services\crypt32[diaglevel]
  Oueries value:
  Oueries value:
                                   HKLM\system\currentcontrolset\services\crypt32[diagmatchanymask]
  Oueries value:
                                    HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
980053277-1733835069-2361817685-1001[profileimagepath]
  Queries value:
                                   HKLM\system\currentcontrolset\control\cmf\config[system]
  Oueries value:
                                   HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
                                   HKLM\software\policies\microsoft\windows\currentversion\internet
  Oueries value:
settings[secureprotocols]
                                    HKCU\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings[secureprotocols]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[secureprotocols]
                                   \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Oueries value:
settings[certificaterevocation]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablekeepalive]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablepassport]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[idnenabled]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[cachemode]
                                    HKLM\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings[enablehttp1_1]
  Queries value:
                                    HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[enablehttp1_1]
                                    HKLM\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings[proxyhttp1.1]
  Queries value:
                                    \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} internet \end{tabular}
settings[proxyhttp1.1]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[proxyhttp1.1]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[enablenegotiate]
                                   \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings[disablebasicoverclearchannel]
                                   HKCU\software\microsoft\internet
  Oueries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
                                   HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main\featurecontrol[feature clientauthcertfilter]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
                                   HKLM\software\microsoft\rpc[maxrpcsize]
  Oueries value:
  Queries value:
                                   HKLM\software\microsoft\sqmclient\windows[ceipenable]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[syncmode5]
                                   Queries value:
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
                                   HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache[signature]
                                   \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \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\cache\content[peruseritem]
  Queries value:
                                   settings\5.0\cache\content[peruseritem]
  Queries value:
HKLM \label{lem:hklm} White the software \label{lklm} White the 
33be-4251-ba85-6007caedcf9d}[category]
  Oueries value:
33be-4251-ba85-6007caedcf9d}[name]
  Oueries value:
33be-4251-ba85-6007caedcf9d}[parentfolder]
  Oueries value:
33be-4251-ba85-6007caedcf9d}[description]
  Oueries value:
33be-4251-ba85-6007caedcf9d}[relativepath]
  Oueries value:
```

33be-4251-ba85-6007caedcf9d}[parsingname]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ for the first bar of the first bar of the formula of the first bar of the first b$ 

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

 $\label{thm:local-base-4251-base-4251-base-6007} HKLM\software\wow6432\node\microsoft\windows\currentversion\explorer\folderdescriptions\folderde$ 

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:

 $\label{local_ham} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\calebox{352481e8-33be-4251-ba85-6007} [local redirectonly]$ 

Queries value:

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

Queries value:

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

Oueries value:

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

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

Queries value:

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

Oueries value:

 $\label{thm:local-basic$ 

Queries value:

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

folders[cache]

Queries value:

 $\label{local-operator} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fitb 32785-65ba-4fcf-9d55-7b8e7f157091 \cite{Control of the Control of the Co$ 

Queries value:

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\soft\windows\currentversion\explorer\folder descriptions \fib32785-66ba-4fcf-9d55-7b8e7f157091\[parentfolder\]$ 

Queries value:

Queries value:

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1} folder \colored \footnote{1} folder \colored \footnote{2} folder \footnote{2} folder \footnote{2} folder \footnote{2} folder \footnote{2} folder \footnote{2} folder \footnote{2} footnote{2} footno$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\ff1b32785-6fba-4fcf-9d55-7b8e7f157091\} [infotip]$ 

Queries value:

 $\label{thm:localized} $HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[localized name]}$ 

Queries value:

 $\label{lem:hkkm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\fifth{1}{5}2785-65ba-4fcf-9d55-7b8e7f157091\fifth{1}{5}[icon]$ 

Queries value:

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f1b32785-b2785$ 

6fba-4fcf-9d55-7b8e7f157091}[localredirectonly]

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries 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:

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

Queries value:

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

folders[local appdata]

Queries value:

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

Queries value:

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

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:

 $\label{lem:hklmsoftwarewow6432node} Hklm\soft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[relativepath]}$ 

Queries value:

 $\label{thm:local-state} $HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[parsingname]} $$$ 

Queries value:

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

Queries value:

Queries value:

 $\label{thm:local-bound} $HKLM \circ two explorer \ends on explorer \ends on the properties of the proper$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\soft\windows\currentversion\explorer\folderdescriptions \currentversion\explorer\folderdescriptions \currentversion\explorer\folderdescription$ 

Queries value:

 $\label{thm:local-bound} $HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[streamresource]$$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\soft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[streamresourcetype]}$ 

Queries value:

 $\label{thm:local-cond} $HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[localredirectonly]}$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\\folderdescriptions\\\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[roamable]$ 

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-bound} $HKLM \cdot software \cdot wow 6432 node : local-bound on the context of the c$ 

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions \currentversion\explorer\folder descriptions \currentversion\explorer\folder descriptions \currentversion\explorer\folder descriptions \currentversion\explorer\folder \currentversion\explorer\folder\fo$ 

Queries value:

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

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

settings\5.0\cache\content[cacheprefix]

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

settings\5.0\cache\content[cachelimit]

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

settings\5.0\cache\cookies[peruseritem]

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

settings\5.0\cache\cookies[peruseritem]

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \cdot \$ 

Oueries value:

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

Queries value:

 $\label{lem:hklm} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \cite{lem:hklm} folder \cite{lem:hklm} fold$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{\{}2b0f765d-c0e9-4171-908e-08a611b84ff6\}\folderdescription\fold$ 

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}[infotip]$ 

Oueries value:

 $\label{localized-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \coe9-4171-908e-08a611b84ff6 \coe12ed name]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}[icon]$ 

Queries value:

 $\label{local-observation} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[security]}$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}[streamresource]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\mbox{windows} currentversion\explorer\folderdescriptions\folder$ 

Queries value:

 $\label{local_ham} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\cdef{folderdescriptions} \cdef{folderdescriptions} \cdef{folderdes$ 

Queries value:

 $\label{thm:local-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \coe9-4171-908e-08a611b84ff6 \coe9-4171$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}[precreate]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{align*.} Which is the sum of the sum of$ 

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}[foldertypeid]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}[initfolderhandler]$ 

Queries value:

 $\label{local-continuous} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}}$ 

folders[cookies]

Queries value:

Queries value:

 $\label{thm:condition} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fol$ 

Queries value

 $\label{local-ham} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\ [parentfolder]$ 

Queries value:

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

Oueries value:

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

Oueries value

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [infotip]$ 

Oueries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdesc$ 

Oueries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdots\folderdes\cdots\folderdes$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[security]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [stream resource]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [stream resource type]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder 6569-4cf6-a03a-e3ef65729f3d \cite{local redirectonly} \end{microsoft}$ 

Queries value:

Oueries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[stream]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [publish \ explorer\ folder \ below \ folder \ fold$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [attributes]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$ 

Queries value:

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

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]

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

settings\5.0\cache\cookies[cachelimit]

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

settings\5.0\cache\history[peruseritem]

 $\label{thm:local_queries} Queries \ value: \\ HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet \\$ 

settings\5.0\cache\history[peruseritem]

Queries value:

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

Queries value:

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

Queries value:

 $\label{linear_ham} HKLM software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \eqref{d9dc8a3b-b784-432e-a781-5a1130a75963} \cite{linear_ham} \eqref{d9dc8a3b-b784-432e-a781-5a1130a$ 

Queries value:

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

Queries value:

 $HKLM\$  software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[relativepath]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[parsingname]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[infotip]

Queries value:

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

```
b784-432e-a781-5a1130a75963}[icon]
  Oueries value:
b784-432e-a781-5a1130a75963}[security]
  Queries value:
b784-432e-a781-5a1130a75963}[streamresource]
  Oueries value:
b784-432e-a781-5a1130a75963}[streamresourcetype]
  Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-d12b, d12b, d24b, d
b784-432e-a781-5a1130a75963}[localredirectonly]
  Queries value:
b784-432e-a781-5a1130a75963}[roamable]
b784-432e-a781-5a1130a75963}[precreate]
  Queries value:
b784-432e-a781-5a1130a75963}[stream]
b784-432e-a781-5a1130a75963}[publishexpandedpath]
b784-432e-a781-5a1130a75963}[attributes]
b784-432e-a781-5a1130a75963}[foldertypeid]
b784-432e-a781-5a1130a75963}[initfolderhandler]
                               \label{local-continuity} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}}
  Queries value:
folders[historv]
  Queries value:
                               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
                               HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\history[cachelimit]
                               HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\domstore[cacherepair]
  Queries value:
                               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachepath]
                               HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
  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]
  Oueries 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]
                               HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
  Queries value:
                               \label{lem:hkcu} \verb+KCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings\5.0\cache\extensible cache\iecompat[cacherepair]
                               HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\iecompat[cachepath]
  Oueries value:
                               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
                               \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
  Queries value:
settings\5.0\cache\extensible cache\iecompat[cachelimit]
                               HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
  Oueries value:
                               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
  Queries value:
                               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
                               HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\ietld[cacheprefix]
```

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\privacie:[cacherepair]

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

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

HKCU\software\microsoft\windows\currentversion\internet

HKCU\software\microsoft\windows\currentversion\internet

Oueries value:

```
Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 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]
 Queries 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]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[mbcsapiforcrack]
                          \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
 Oueries value:
settings[utf8servernameres]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablereadrange]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketsendbufferlength]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketreceivebufferlength]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxhttpredirects]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsper1_0server]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[serverinfotimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connecttimeout]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connecttimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connectretries]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connectretries]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendtimeout]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[receivetimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablentlmpreauth]
                          \label{lem:hkcu} \verb+KKCU \software \verb+microsoft + windows \verb+current version \verb+\internet+ \\
 Queries value:
settings[scavengecachelowerbound]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelifetime]
 Queries value:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
 Queries value:
                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[ftpdefaultexpirytimesecs]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Queries value:
HKLM\svstem\currentcontrolset\services\winsock2\parameters[namespace callout]
 Queries value:
                          HKLM\software\wow6432node\microsoft\internet
```

```
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[cgu1eed.exe]
                               HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000003[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000004[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000006[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[packedcatalogitem]
                                HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablecachingofsslpages]
  Queries value:
                               HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
                                HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[leashlegacycookies]
                                HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dialupuselansettings]
  Queries value:
                               HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
                               HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[sendextracrlf]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog_entries\00000000008[packedcatalogitem]
  Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ (000000000009[packed catalog item]) \ details \ de
  Queries value:
HKLM\svstem\currentcontrolset\services\winsock2\parameters\namespace catalog5[serial access num]
  Queries value:
                               HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
                                HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasshttpnocachecheck]
  Queries value:
                               settings[bypasshttpnocachecheck]
  Queries value:
                               HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
                               HKLM\software\wow6432node\microsoft\windows\currentyersion\internet
  Oueries value:
settings[bypasssslnocachecheck]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
  Oueries value:
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:
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]]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
  Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerinfo]
                                HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[dontusednsloadbalancing]
                                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
settings[dontusednsloadbalancing]
```

Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[sharecredswithwinhttp] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[mimeexclusionlistforcache] Oueries value:  $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace \_catalog5 \ catalog\_entries \ 000000000002 [library path]$ Oueries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[providerid] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[addressfamily] Oueries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[enabled] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[headerexclusionlistforcache] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[dnscacheenabled] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[dnscacheentries] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[dnscachetimeout] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[warnonpost] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[warnalwaysonpost] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[warnonzonecrossing] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[warnonbadcertrecving] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000002[version] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[storesserviceclassinfo] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000003[librarypath] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[displaystring] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[warnonpostredirect] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[alwaysdrainonredirect] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonhttpstohttpredirect] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings[tcpautotuning] Oueries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[addressfamily] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[supportednamespace] Oueries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog 5 \setminus catalog\_entries \setminus 0000000000003 [enabled]$ Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[version] Queries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[providerinfo] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000004[librarypath] Queries value:  $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 000000000004 \ [displaystring]$ Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog S \setminus catalog\_entries \setminus 0000000000004 [providerid]$ Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[addressfamily] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[supportednamespace] Queries value:  $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ set alog\_entries \ (0000000000004 [enabled]) \ details \ d$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[version]

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap services \setminus mame space\_catalog \\ \setminus catalog\_entries \setminus 00000000000004[provider info]$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[storesserviceclassinfo]

Oueries value:

Queries value:

```
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ (catalog\_entries \ 00000000005[library path]) \ (catalog\_entries \ (catalog entries \ (catalog entries \ 
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
   Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog S \setminus catalog\_entries \setminus 0000000000005[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
   Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000005 [supported name space]]
   Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus names pace\_catalog \\ \setminus catalog\_entries \setminus 0000000000005 [enabled]
   Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_entries\00000000005[storesserviceclassinfo]
   Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap services \setminus mame space\_catalog \\ \setminus catalog\_entries \setminus 0000000000005[provider info]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
   Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog S \setminus catalog\_entries \setminus 0000000000006[providerid]
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 \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap services \setminus ser
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
   Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
   Queries value:
                                                     HKLM\system\currentcontrolset\services\winsock\parameters[transports]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
                                                     HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
   Queries value:
                                                     HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
   Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
                                                     HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\wpad[wpadoverride]
   Queries value:
                                                     \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
settings[enableautodial]
   Queries value:
                                                     HKCU\software\microsoft\windows\currentversion\internet
settings[nonetautodial]
                                                      HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[globaluseroffline]
                                                      HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[badproxyexpirestime]
   Queries value:
                                                     HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version\\| internet
settings[disablebranchcache]
                                                     HKLM\software\wow6432node\microsoft\internet
   Oueries value:
explorer\main\featurecontrol\feature_http_username_password_disable[cgu1eed.exe]
                                                     HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature http username password disable[*]
   Queries value:
                                                     HKLM\software\wow6432node\microsoft\tracing[enableconsoletracing]
   Queries value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[enablefiletracing]
   Queries value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[filetracingmask]
   Oueries value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[enableconsoletracing]
   Queries value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[consoletracingmask]
   Queries value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[maxfilesize]
   Oueries value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[filedirectory]
                                                     HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\profilelist[programdata]
   Queries value:
                                                      HKLM\software\microsoft\sqmclient\windows\disabledprocesses[dd79cc82]
```

Oueries value:

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

Oueries value:

HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]

Queries value:

HKLM\software\wow6432node\microsoft\tracing\cgu1eed\_rasmancs[enablefiletracing]

Oueries value:

 $HKLM \verb|\software| \verb|\wow6432| node \verb|\microsoft| tracing \verb|\cgu1eed_rasmancs[filetracingmask]|$ 

Oueries value:

HKLM\software\wow6432node\microsoft\tracing\cgu1eed\_rasmancs[enableconsoletracing]

Oueries value:

HKLM\software\wow6432node\microsoft\tracing\cgu1eed\_rasmancs[consoletracingmask]

Oueries value:

HKLM\software\wow6432node\microsoft\tracing\cgu1eed\_rasmancs[maxfilesize]

Queries value:

HKLM\software\wow6432node\microsoft\tracing\cgu1eed\_rasmancs[filedirectory]

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

settings[proxysettingsperuser]

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

settings[migrateproxy]

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

settings[proxyenable]

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

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

settings\connections[savedlegacysettings]

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

settings\connections[defaultconnectionsettings]

Queries value:

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

Oueries value:

Queries value:

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

Oueries value:

 $\label{thm:local-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \equal 1777 f761-68 ad-4d8a-87 bd-30 b759 fa 33 dd \equal [description]$ 

Queries value:

 $\label{local-ham} $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}\[relative path]$ 

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(1777f761-68ad-4d8a-87bd-30b759fa33dd)\f(10calizedname)\f(1777f761-68ad-4d8a-87bd-30b759fa33dd)\f(10calizedname)\f(1777f761-68ad-4d8a-87bd-30b759fa33dd)\f(10calizedname)\f(1777f761-68ad-4d8a-87bd-30b759fa33dd)\f(10calizedname)\f(1777f761-68ad-4d8a-87bd-30b759fa33dd)\f(10calizedname)\f(1777f761-68ad-4d8a-87bd-30b759fa33dd)\f(10calizedname)\f(1777f761-68ad-4d8a-87bd-30b759fa33dd)\f(10calizedname)\f(1777f761-68ad-4d8a-87bd-30b759fa33dd)\f(10calizedname)\f(1777f761-68ad-4d8a-87bd-30b759fa33dd)\f(10calizedname)\f(1777f761-68ad-4d8a-87bd-30b759fa33dd)\f(10calizedname)\f(1777f761-68ad-4d8a-87bd-30b759fa33dd)\f(10calizedname)\f(1777f761-68ad-4d8a-87bd-30b759fa33dd)\f(10calizedname)\f(1777f761-68ad-4d8a-87bd-30b759fa33dd)\f(10calizedname)\f(1777f761-68ad-4d8a-87bd-30b759fa33dd)\f(1777f761-68ad-4d8a$ 

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

Queries value:

 $\label{thm:ham} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \cal{thm:ham} \footnote{1777f761-68ad-4d8a-87bd-30b759fa33dd} \cite{10calredirectonly} \cite{10calredirectonly} \cite{10calredirectonly} \end{tikzpicture}$ 

Queries value:

Oueries value:

Queries value:

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

Queries value:

```
68ad-4d8a-87bd-30b759fa33dd}[publishexpandedpath]
  Oueries value:
68ad-4d8a-87bd-30b759fa33dd}[attributes]
  Oueries value:
68ad-4d8a-87bd-30b759fa33dd}[foldertypeid]
  Oueries value:
68ad-4d8a-87bd-30b759fa33dd}[initfolderhandler]
                                   \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ user shell
  Oueries value:
folders[favorites]
  Queries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\appcompatflags[{d97b6486-0cfa-44d8-acc2-0f8b5941e889}]
                                   HKCU\software\microsoft\windows
  Queries value:
nt\currentversion\appcompatflags[{d97b6486-0cfa-44d8-acc2-0f8b5941e889}]
                                   HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\appcompatflags[{44480e68-dfd5-435f-bdfe-b8246fc9f90f}]
                                   HKCU\software\microsoft\windows
  Queries value:
nt \verb|\currentversion| app compatflags[\{44480e68-dfd5-435f-bdfe-b8246fc9f90f\}]|
                                   HKLM\software\wow6432node\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_mime_handling[cgu1eed.exe]
                                   HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_mime_handling[*]
                                   HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
  Queries value:
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
  Queries value:
\label{thm:local_transform} \parbox{$\tt HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]$} \parbox{$\tt HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]$} \parbox{$\tt HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]$} \parbox{$\tt HKLM\system\currentcontrolset\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\services\s
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [prioritize record data]
  Queries value:
HKLM \ system \ current control set \ services \ dns cache \ parameters [allow unqualified query]
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [screen badtlds]
HKLM\svstem\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
                                   HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
  Oueries value:
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [dnssecurename query fallback]
  Queries value:
Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[directaccessquervorder]
  Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[quervipmatching]
                                   HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
  Queries value:
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
  Oueries value:
```

```
Oueries 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]
 Oueries 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:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
                        HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
 Queries value:
                        HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
 Queries value:
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout]
                        HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
 Oueries value:
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [use compartments]
HKLM\svstem\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
                        HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_unc_savedfilecheck[cgu1eed.exe]
                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[*]
 Queries value:
                        HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
                        HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\0[flags]
                        HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\1[flags]
 Queries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[flags]
                        HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\3[flags]
 Oueries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[flags]
 Queries value:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[cgu1eed.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[cgu1eed.exe]
 Oueries value:
                            HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
                            HKLM\software\wow6432node\microsoft\windows
 Oueries value:
nt\currentversion\aedebug[debugger]
 Queries value:
                            HKLM\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
 Queries value:
                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[createuricachesize]
                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[createuricachesize]
                            HKLM\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[enablepunycode]
                            HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablepunycode]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zonemap[autodetect]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\3[1a10]
                            HKCU\software\microsoft\windows
 Queries value:
\verb|nt\currentversion\appcompatflags[showdebuginfo]|\\
                            HKLM\software\wow6432node\microsoft\windows
 Queries value:
nt\currentversion\compatibility32[rundll32]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache[signature]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\lowcache\content[peruseritem]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\lowcache\content[cacheprefix]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\content[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\lowcache\cookies[peruseritem]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\cookies[cacheprefix]
 Queries value:
                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings\5.0\lowcache\cookies[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\lowcache\history[peruseritem]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\history[cacheprefix]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings\5.0\lowcache\history[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\lowcache\extensible cache\feedplat[cacherepair]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\feedplat[cachepath]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\feedplat[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\lowcache\extensible cache\feedplat[cachelimit]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\feedplat[cacheoptions]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\iecompat[cacherepair]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\lowcache\extensible cache\iecompat[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\lowcache\extensible cache\iecompat[cacheprefix]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\iecompat[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\lowcache\extensible cache\iecompat[cacheoptions]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\lowcache\extensible cache\ietld[cacherepair]
 Queries 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:
                            \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\lowcache\extensible cache\ietld[cachelimit]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\ietld[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\lowcache\extensible cache\privacie:[cacherepair]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
```

settings\5.0\lowcache\extensible cache\privacie:[cachepath]

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

settings\5.0\lowcache\extensible cache\privacie:[cacheprefix] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\lowcache\extensible cache\privacie:[cachelimit] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\lowcache\extensible cache\privacie:[cacheoptions] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_disable\_unicode\_handle\_closing\_callback[rundll32.exe] HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a66e19e6] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[searchlist] Queries value: e1e01c1f69b5}[enabledhcp] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[registrationenabled] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[registeradaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[domain] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[dhcpdomain] Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[dhcpv6domain] Queries value: e1e01c1f69b5}[nameserver] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[nameserver] Queries value: e1e01c1f69b5}[dhcpnameserver] Oueries value: 806e6f6e6963}[enabledhcp] Queries value: 806e6f6e6963}[registrationenabled] Oueries value: 806e6f6e6963}[registeradaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[domain] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpdomain] Oueries value: 806e6f6e6963}[nameserver] Queries value: 806e6f6e6963}[dhcpnameserver] HKLM\system\currentcontrolset\services\tcpip\linkage[bind] Oueries value: Queries value: e1e01c1f69b5}[queryadaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[disableadapterdomainname] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[registrationmaxaddresscount]

Queries value:

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

Queries value:

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

Oueries value:

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

```
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[disableadapterdomainname]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[disabledynamicupdate]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[enableadapterdomainnameregistration]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[registrationmaxaddresscount]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[maxnumberofaddressestoregister]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
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]
   Queries value:
                                                  HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
   Oueries value:
                                                 HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
   Queries value:
                                                  HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
   Queries value:
                                                  HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
                                                  Queries value:
   Queries value:
                                                  HKCU\software\microsoft\internet explorer\ietld[ietldversionhigh]
   Queries value:
                                                  HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6[winsock 2.0 provider id]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
                                                 HKLM\software\wow6432node\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_zone_elevation[cgu1eed.exe]
                                                 HKLM\software\wow6432node\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_zone_elevation[*]
                                                 \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{microsoft} \windows \current version \hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_h
settings\zones\3[{aeba21fa-782a-4a90-978d-b72164c80120}]
   Queries value:
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings[privacyadvanced]
                                                 HKLM\system\currentcontrolset\control\session
  Sets/Creates value:
manager[pendingfilerenameoperations]
   Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\run[1h6wzb8fvvuwzwwulvatv]
   Sets/Creates value:
                                                  \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings\zones\0[1409]
   Sets/Creates value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1609]
  Sets/Creates value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1406]
   Sets/Creates value:
                                                  \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings\lockdown_zones\
                                                1Γ14061
                                                 \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
   Sets/Creates value:
settings\lockdown_zones\2[1406]
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Sets/Creates value:
settings\lockdown zones\3[1406]
                                                 \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
   Sets/Creates value:
settings\lockdown_zones\4[1406]
                                                 HKCU\software\microsoft\internet
   Sets/Creates value:
explorer\phishingfilter[shownservicedownballoon]
                                                 HKCU\software\microsoft\internet
   Sets/Creates value:
explorer\recovery[clearbrowsinghistoryonexit]
   Sets/Creates value:
                                                 \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[globaluseroffline]
   Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[enablefiletracing]
HKLM \label{lem:hklm} LS = \frac{1}{2} [enable \label{lem:hklm} a pi32 [enable \label{lem:hklm} enable \label{lem:hklm} lS = \frac{1}{2} [enable \label{lem:hklm} enable \label{lkm} enabl
   Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[filetracingmask]
   Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[consoletracingmask]
   Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[maxfilesize]
   Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\cgu1eed_rasapi32[filedirectory]
   Sets/Creates value:
```

 $HKLM \verb|\software| wow 6432 node \verb|\microsoft| tracing \verb|\cgu1eed_rasmancs[enable file tracing]| \\$ 

Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\cgu1eed\_rasmancs[enableconsoletracing] Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\cgu1eed\_rasmancs[filetracingmask] Sets/Creates value:  $HKLM \verb|\software| wow 6432 node \verb|\microsoft| tracing \verb|\cgu1eed_rasmancs[consoletracing mask]| \\$ Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\cgu1eed\_rasmancs[maxfilesize] Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\cgu1eed\_rasmancs[filedirectory] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings[enablehttp1\_1] Value changes: HKCU\software\microsoft\windows\currentversion\internet 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:  $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ settings[warnonintranet] Value changes:  $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ settings\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:  $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ settings\zones\2[1409] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\zones\2[1609] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[1406] Value changes:  $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ settings\zones\3[1409] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\zones\3[1609] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\zones\3[1406]  $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Value changes: settings\zones\4[1409] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\zones\4[1609] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\zones\4[1406] Value changes: HKCU\software\microsoft\internet explorer\phishingfilter[enabledv8] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[proxyenable] Value changes:  $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}$ 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] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings[globaluseroffline]