Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details Host: mag2, Sample ID: 3304, Task ID: 724

Task ID: 724 Risk Level: 10

Date Processed: 2016-05-18 10:30:53 (UTC)

Processing Time: 7.56 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\709ce21bcb87f234c01594e44f12936e.exe"

Sample ID: Type: basic admin Owner:

709ce21bcb87f234c01594e44f12936e Label:

Date Added: 2016-05-18 10:30:48 (UTC)

PE32:win32:gui File Type: File Size: 34304 bytes

709ce21bcb87f234c01594e44f12936e MD5:

04cb60d93c513853e9505a34da81866709be62a884d88383d714227d0780911d SHA256:

Description: None

Pattern Matching Results

10 Creates malicious events: Beebone [Trojan]

Checks task list from command line

3 Long sleep detected

4 Terminates process under Windows subfolder

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

C:\WINDOWS\Temp\709ce21bcb87f234c01594e44f12936e.exe Creates process:

["c:\windows\temp\709ce21bcb87f234c01594e44f12936e.exe"]

C:\WINDOWS\system32\cmd.exe ["C:\WINDOWS\system32\cmd.exe" /c Creates process:

tasklist&&del 709ce21bcb87f234c01594e44f12936e.exel

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

Loads service: RASMAN [C:\WINDOWS\system32\svchost.exe -k netsvcs] Terminates process: C:\WINDOWS\Temp\709ce21bcb87f234c01594e44f12936e.exe

Terminates process: C:\WINDOWS\system32\tasklist.exe Terminates process: C:\WINDOWS\system32\cmd.exe

Named Object Events

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

1957994488-1003

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

1957994488-1003

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

1957994488-1003

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

1957994488-1003 Creates mutex:

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

\BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-Creates mutex: 507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003 \BaseNamedObjects\c:!documents and settings!admin!local Creates mutex:

settings!temporary internet files!content.ie5!

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

settings!history!history.ie5!

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

Creates mutex: \BaseNamedObjects\ZoneAttributeCacheCounterMutex \BaseNamedObjects\ZonesCacheCounterMutex Creates mutex: Creates mutex: \BaseNamedObjects\ZonesLockedCacheCounterMutex

Creates mutex: \BaseNamedObjects\SHIMLIB_LOG_MUTEX

Creates event: \BaseNamedObjects\userenv: User Profile setup event

\BaseNamedObjects\C:?WINDOWS?TEMP?709CE21BCB87F234C01594E44F12936E.EXE Creates semaphore:

Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1} \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D} Creates semaphore: Creates semaphore: \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}

File System Events

Opens: C:\WINDOWS\Prefetch\709CE21BCB87F234C01594E44F129-2B2FC41B.pf

Opens: C:\Documents and Settings\Admin C:\WINDOWS\system32\msvbvm60.dll Opens: C:\WINDOWS\system32\imm32.dll Opens: Opens: C:\WINDOWS\system32\rpcss.dll

```
C:\WINDOWS\system32\MSCTF.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\sxs.dll
                         C:\WINDOWS\system32\MSCTFIME.IME
 Opens:
 Opens:
                         C:\WINDOWS\Temp\709ce21bcb87f234c01594e44f12936e.exe
 Opens:
                         C:\
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Manifest
                         C:\WINDOWS\system32\urlmon.dll.123.Config
 Opens:
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
 Opens:
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
                         C:\WINDOWS\WindowsShell.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\WindowsShell.Config
                         C:\WINDOWS\system32\wininet.dll.123.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\wininet.dll.123.Config
                         C:\WINDOWS\system32\shell32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Config
 Opens:
                         C:\WINDOWS\system32\comctl32.dll
                         C:\WINDOWS\system32\comctl32.dll.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Config
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History
                         C:\Documents and Settings\Admin\Local Settings\History\History.IE5
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
                         C:\Documents and Settings\Admin\Cookies
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Cookies\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\index.dat
                         C:\WINDOWS\system32\ws2_32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\ws2help.dll
 Opens:
                         C:\WINDOWS\system32\rasapi32.dll
 Opens:
                         C:\WINDOWS\system32\rasman.dll
 Opens:
                         C:\WINDOWS\system32\netapi32.dll
 Opens:
                         C:\WINDOWS\system32\tapi32.dll
 Opens:
                         C:\WINDOWS\system32\rtutils.dll
 Opens:
                         C:\WINDOWS\system32\winmm.dll
                         C:\WINDOWS\system32\TAPI32.dll.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\TAPI32.dll.124.Config
 Opens:
                         C:\AUTOEXEC.BAT
                         C:\Documents and Settings\All Users\Application
 Opens:
Data\Microsoft\Network\Connections\Pbk
 Opens:
                         C:\WINDOWS\system32\ras
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Microsoft\Network\Connections\Pbk\
                         C:\WINDOWS\system32\sensapi.dll
 Opens:
                         C:\WINDOWS\system32\mswsock.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\rasadhlp.dll
 Opens:
                         C:\WINDOWS\system32\dnsapi.dll
                         C:\WINDOWS\system32\iphlpapi.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\drivers\etc\hosts
 Opens:
                         C:\WINDOWS\system32\rsaenh.dll
 Opens:
                         C:\WINDOWS\system32\crypt32.dll
 Opens:
                         C:\WINDOWS\system32\hnetcfg.dll
 Opens:
                         C:\WINDOWS\system32\msv1 0.dll
 Opens:
                         C:\WINDOWS\system32\wshtcpip.dll
 Opens:
                         C:\WINDOWS\system32\ieframe.dll
 Opens:
                         C:\WINDOWS\system32\clbcatq.dll
 Opens:
                         C:\WINDOWS\system32\comres.dll
                         C:\WINDOWS\Registration\R00000000007.clb
 Opens:
 Opens:
                         C:\Program Files\Internet Explorer\iexplore.exe
 Opens:
                         C:\WINDOWS\system32\ieframe.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\ieframe.dll.123.Config
 Opens:
                         C:\WINDOWS\system32\en-US\ieframe.dll.mui
                         C:\WINDOWS\system32
 Opens:
 Opens:
                         C:\WINDOWS
 Opens:
                         C:\WINDOWS\system32\setupapi.dll
                         C:\WINDOWS\system32\cmd.exe
 Opens:
 Opens:
                         C:\WINDOWS\AppPatch\sysmain.sdb
 Opens:
                         C:\WINDOWS\AppPatch\systest.sdb
                         C:\WINDOWS\system32\cmd.exe.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf
 Opens:
                         C:\WINDOWS\WINHELP.INI
 Opens:
 Opens:
                         C:\WINDOWS\AppPatch
 Opens:
                         C:\WINDOWS\system32\wbem
 Opens:
                         C:\WINDOWS\WinSxS
 Opens:
                         C:\WINDOWS\system32\ntdll.dll
 Opens:
                         C:\WINDOWS\svstem32\kernel32.dll
 Opens:
                         C:\WINDOWS\system32\unicode.nls
```

C:\WINDOWS\system32\locale.nls Opens: Opens: C:\WINDOWS\system32\sorttbls.nls Opens: C:\WINDOWS\system32\msvcrt.dll Opens: C:\WINDOWS\system32\user32.dll Opens: C:\WINDOWS\system32\gdi32.dll Opens: C:\WINDOWS\system32\shimeng.dll Opens: C:\WINDOWS\AppPatch\AcGenral.dll Opens: C:\WINDOWS\system32\advapi32.dll Opens: C:\WINDOWS\system32\rpcrt4.dll Opens: C:\WINDOWS\system32\secur32.dll Opens: C:\WINDOWS\svstem32\ole32.dll Opens: C:\WINDOWS\system32\oleaut32.dll Opens: C:\WINDOWS\system32\msacm32.dll Opens: C:\WINDOWS\system32\version.dll Opens: C:\WINDOWS\system32\shlwapi.dll Opens: C:\WINDOWS\system32\userenv.dll Opens: C:\WINDOWS\system32\uxtheme.dll Opens: C:\WINDOWS\system32\ctype.nls Opens: C:\WINDOWS\system32\sortkey.nls Opens: C:\WINDOWS\system32\apphelp.dll Opens: C:\WINDOWS\system32\wbem\wmic.exe Opens: C:\Documents and Settings

Opens: C:\WINDOWS\system32\tasklist.exe

Opens: C:\WINDOWS\system32\tasklist.exe.Manifest Opens: C:\WINDOWS\Prefetch\TASKLIST.EXE-10D94B23.pf

Opens: C:\WINDOWS\system32\wbem\framedyn.dll Opens: C:\WINDOWS\system32\dbghelp.dll Opens: C:\WINDOWS\system32\winlogon.exe Opens: C:\WINDOWS\svstem32\xpsp2res.dll Opens: C:\WINDOWS\system32\wbem\wbemprox.dll Opens: C:\WINDOWS\system32\wbem\wbemcomn.dll Opens: C:\WINDOWS\system32\winsta.dll Opens: C:\WINDOWS\system32\wbem\wbemsvc.dll Opens: C:\WINDOWS\system32\wbem\fastprox.dll Opens: C:\WINDOWS\system32\msvcp60.dll Opens: C:\WINDOWS\system32\ntdsapi.dll

Reads from: C:\WINDOWS\Temp\709ce21bcb87f234c01594e44f12936e.exe

Reads from: C:\AUTOEXEC.BAT

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

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

Reads from: C:\WINDOWS\Registration\R00000000007.clb

Reads from: C:\WINDOWS\system32\cmd.exe

Reads from: C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf

Network Events

DNS query: domai.7dns.org 8.8.8.8:53 Sends data to: 0.0.0.0:0 Receives data from:

Windows Registry Events

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

folders

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

Creates key: HKLM\software\microsoft\tracing

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

folders

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

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

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

settings\connections

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

awareness

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

Creates key:

HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\0000000000008307

Creates kev: HKI M\software\microsoft\windows\currentversion\shell extensions\blocked Creates key: HKCU\software\microsoft\windows\currentversion\shell extensions\blocked Creates key: HKLM\software\microsoft\windows\currentversion\shell extensions\cached HKCU\software\microsoft\windows\currentversion\shell extensions\cached Creates key:

Creates key:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-

806d6172696f}\

Creates key: HKCU\software\microsoft\visual basic\6.0

Creates key: HKCU\software

HKCU\software\microsoft Creates key:

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

HKCU\software\microsoft\multimedia\audio compression manager\ Creates key: Creates key: HKCU\software\microsoft\multimedia\audio compression manager\msacm Creates key: HKCU\software\microsoft\multimedia\audio compression manager\priority v4.00

Creates kev: HKLM\software\microsoft\wbem\cimom

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

settings[proxyserver]

Deletes value:

HKCU\software\microsoft\windows\currentversion\internet

settings[proxyoverride]

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

settings[autoconfigurl]

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

options\709ce21bcb87f234c01594e44f12936e.exe

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

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

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

options\gdi32.dll

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

options\user32.dll

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

Opens key: $\label{lem:hklm} \mbox{HKLM} \mbox{$\stackrel{\mbox{$\sim$}}{\mbox{$\sim$}}$ file execution}$

options\imm32.dll

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

options\ntdll.dll

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

options\kernel32.dll

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

options\secur32.dll

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

options\rpcrt4.dll

Opens key: options\advapi32.dll

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

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

Opens key: options\msvcrt.dll

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

options\ole32.dll

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

options\oleaut32.dll

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

options\msvbvm60.dll

Opens key: HKLM\system\currentcontrolset\control\error message instrument\ Opens key: HKLM\system\currentcontrolset\control\error message instrument Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ gre_initialize$ Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32 HKLM\software\microsoft\windows nt\currentversion\ime compatibility Opens key:

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

HKLM\ Opens key:

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

HKLM\software\microsoft\ole Opens kev:

Opens key: HKCR\interface

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

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

Opens key:

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

Opens key: HKCU\control panel\desktop

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

options\msctf.dll

Opens kev:

HKLM\software\microsoft\ctf\compatibility\709ce21bcb87f234c01594e44f12936e.exe

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

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

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

options\sxs.dll

Opens key: HKLM\system\setup

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

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

options\version.dll

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

options\msctfime.ime

Opens key: HKCU\software\microsoft\ctf

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

Opens key: HKLM\system\currentcontrolset\control\nls\codepage

Opens kev: HKLM\software\microsoft\vba\monitors

Opens key: HKLM\system\currentcontrolset\services\disk\enum

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

options\shlwapi.dll

Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\normaliz.dll

Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution$ options\iertutil.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key:

options\urlmon.dll

Opens key:

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

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

options\comctl32.dll

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

options\wininet.dll

Opens key: HKCU\software\classes\

Opens key: HKCU\software\classes\protocols\name-space handler\

Opens key: HKCR\protocols\name-space handler

Opens key: HKCU\software\classes\protocols\name-space handler

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

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

settings

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

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

settings\

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

 $\label{lem:hklm} \mbox{HKLM} \mbox{$\operatorname{KLM}\ensuremath{\mbox{\mbox{W}}} explorer \mbox{main feature} ontrol $$ \mbox{$\operatorname{LM}\ensuremath{\mbox{$\mbox{$W$}}} explorer \mbox{$\operatorname{Months}\ensuremath{\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$$W$}}} explorer} \mbox{$\mbox{$\mbox{$\mbox{$$\mbox{$$\mbox{$$$$}} explorer} \mbox{$\mbox{$\mbox{$$$$}} explorer} \mbox{$\mbox{$\mbox{$$$$}} explorer \mbox{$\mbox{$\mbox{$$$$}} explorer \mbox{$\mbox{$$$$} explorer} \mbox{$\mbox{$\mbox{$$$}} explorer} \mbox{$\mbox{$\mbox{$$$}} explorer \mbox{$\mbox{$$$$} explorer} \mbox{$\mbox{$\mbox{$$$}} explorer \mbox{$\mbox{$$$$} explorer} \mbox{$\mbox{$\mbox{$$$}} explorer \mbox{$\mbox{$$$$} explorer} \mbox{$\mbox{$\mbox{$$$}} explorer \mbox{$\mbox{$$$$}} explorer \mbox{$\mbox{$$$$} explorer} \mbox{$\mbox{$\mbox{$$$}} explorer} \mbox{$\mbox{$\mbox{$$}} explorer \mbox{$\mbox{$$$}} explorer \mbox{$\mbox{$\mbox{$$$}} explorer \mbox{$\mbox{$$$}} explorer \mbox{$\mbox{$\mbox{$$$}} explorer \mbox{$\mbox{$$$}} explorer \mbox{$\mbox{$\mbox{$$$}} explorer \mbox{$\mbox{$$$}} explorer \mbox{$\mbox{$$$} explorer \mbox{$\mbox{$$$} explorer \mbox{$\mbox{$$$}} explorer \mbox{$\mbox{$$$} explorer \mbox{$\mbox{$$} explorer \mbox{$\mbox{$$$} explorer \mbox{$\mbox{$$}$ Opens key: Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\

Opens key:

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

settings\zonemap\domains\

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

settings\zonemap\ranges\

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

settings\zonemap\ranges\

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

Opens key: HKLM\system\currentcontrolset\control\wmi\security

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

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

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

settings\5.0\cache

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

settings\5.0\cache

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

settings\5.0\cache\content

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

settings\5.0\cache\content

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

options\shell32.dll

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

settings\5.0\cache\cookies Opens key:

HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies

Opens key:

HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\history

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

settings\5.0\cache\history HKLM\software\microsoft\rpc\pagedbuffers Opens key:

Opens key: HKLM\software\microsoft\rpc

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

options\709ce21bcb87f234c01594e44f12936e.exe\rpcthreadpoolthrottle Opens key: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKLM\system\currentcontrolset\control\computername

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

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

settings\5.0\cache\extensible cache

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

settings\5.0\cache\extensible cache\domstore

```
Opens key:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat
 Opens key:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat
                        HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0\cache\extensible cache\ietld
 Opens key:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407
 Opens key:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413
                        HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0\cache\extensible cache\privacie:
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
                        HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_bufferbreaking_818408
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature bufferbreaking 818408
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
                        HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
 Opens key:
                        HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
 Opens key:
                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
                        HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                        HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                        HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                        HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
                        HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens kev:
                        HKLM\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature\_allow\_long\_international\_file names|\\
                        HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens kev:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
                        HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature disable unicode handle closing callback
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
                        HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
 Opens key:
                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
 Opens key:
                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
 Opens key:
                        HKLM\system\currentcontrolset\services\winsock2\parameters
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
 Opens kev:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001
 Opens key:
Opens kev:
```

Opens key:

Opens kev:

Opens kev:

Opens kev:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008 Opens kev:

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000011 Opens key:

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

Opens key:

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615

HKLM\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_http_username_password_disable

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_http_username_password_disable

 $\label{thm:local_hammon} \mbox{HKLM\software\mbox{\sc hickness} in \sc hickness} \mbox{\sc hickness} \mb$ Opens key:

options\netapi32.dll

HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\rasman.dll

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

Opens key:

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

Opens key: options\winmm.dll

HKLM\software\microsoft\windows nt\currentversion\drivers32 Opens key:

Opens key:

HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm

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

options\tapi32.dll

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

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

options\rasapi32.dll

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

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

options\userenv.dll

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

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

folders

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist HKLM\system\currentcontrolset\control\session manager\environment Opens key:

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

Opens key: HKU\

 $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus profile list \setminus s-1-5-21-1000 + (1-5)$ Opens key:

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

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

options\sensapi.dll

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

filters\rpa

Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\http

filters\rpa

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_include_port_in_spn_kb908209

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_include_port_in_spn_kb908209 HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_mime_handling

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_mime_handling

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

HKCU\software\microsoft\windows\currentversion\internet

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

Opens key:

Opens key:

settings\lockdown_zones\2

settings\lockdown_zones\2

```
Opens key:
                                                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
                                                           HKCU\software\microsoft\windows\currentversion\internet
    Opens key:
settings\lockdown_zones\3
                                                          HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\lockdown_zones\3
   Opens key:
                                                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
    Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
                                                          HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\4
   Opens key:
                                                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
    Opens key:
                                                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
                                                          HKLM\software\microsoft\internet
   Opens kev:
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
    Opens key:
                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dnsapi.dll
    Opens key:
                                                           HKLM\system\currentcontrolset\services\dnscache\parameters
    Opens key:
                                                           HKLM\software\policies\microsoft\windows nt\dnsclient
    Opens key:
                                                           HKLM\system\currentcontrolset\services\tcpip\parameters
    Opens key:
                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iphlpapi.dll
                                                           HKLM\system\currentcontrolset\services\tcpip\linkage
    Opens key:
    Opens key:
                                                           HKLM\system\currentcontrolset\services\tcpip\parameters\
    Opens key:
                                                           HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
    Opens key:
                                                           HKLM\system\currentcontrolset\services\netbt\parameters
    Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}
    Opens key:
                                                           HKLM\software\policies\microsoft\system\dnsclient
    Opens key:
                                                           HKLM \ software \ microsoft \ cryptography \ defaults \ provider \ microsoft \ strong
cryptographic provider
    Opens key:
                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rsaenh.dll
                                                           HKLM\software\microsoft\rpc\securityservice
    Opens key:
    Opens key:
                                                           HKLM\software\policies\microsoft\cryptography
    Opens key:
                                                           HKLM\system\currentcontrolset\control\securityproviders
    Opens key:
                                                           {\tt HKLM \ } system \verb|\ current control \verb|\ lsa \ | sspicache \\
    Opens key:
                                                           HKLM\software\microsoft\cryptography
                                                           HKLM\software\microsoft\cryptography\offload
    Opens kev:
                                                           HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll
    Opens key:
    Opens key:
                                                           HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll
    Opens key:
                                                           HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll
    Opens key:
                                                           \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution
options\hnetcfg.dll
    Opens kev:
                                                           HKLM\svstem\currentcontrolset\services\winsock\parameters
    Opens key:
                                                           HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
    Opens key:
                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msv1_0.dll
    Opens key:
                                                           HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
    Opens key:
                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wshtcpip.dll
    Opens key:
                                                           HKLM\system\currentcontrolset\services\netbt\linkage
    Opens kev:
HKCU\software\microsoft\windows\currentversion\explorer
    Opens key:
    Opens key:
                                                           HKLM\software\microsoft\windows\currentversion\explorer
    Opens key:
                                                           HKLM\software\microsoft\windows\currentversion\policies\explorer
    Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\policies\explorer
    Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace
HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ 'desktop \ 'namespace \ '\{11016101-e366-4d22-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d1016101-e366-d10161001-e366-d1016101-e366-d10161001-e366-d10161001-e366-d10161001-e366-d10161001-e366-d10161001-e366-d10161001-e366-d10161001-e366-
bc06-4ada335c892b}
    Opens key:
ba4f-00a0c91eedba}
    Opens key:
HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ 'desktop \ 'namespace \ '{450d8fba-ad25-11d0-desktop} \ 'namespace' \ 'namespac
98a8-0800361b1103}
    Opens key:
HKLM \label{lem:hklm} Which is the statement of the sta
9f08-00aa002f954e}
    Opens key:
-HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{e17d4fc0-5564-11d1
83f2-00a0c90dc849}
    Opens key:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \desktop \names pace \end{tabular} \label{lem:hkcu}
    Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\explorer\
```

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ lex plorer \ session in follow 00000000000307 \ desktop \ names pace$

Opens key: HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder

Opens key: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder

Opens key: HKCU\software\classes\clsid\{208d2c60-3aea-1069-a2d7-

08002b30309d}\shellfolder

 $Opens~key: \\ HKCR\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\) shell folder$

Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\shellfolder

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder

Opens kev:

a2ea-08002b30309d}

Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\inprocserver32

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\apphelp.dll

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

Opens key: HKLM\software\microsoft\com3

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

options\comres.dll

 $Opens\ key: \\ HKLM\software\microsoft\windows\ nt\currentversion\sim ge \ file\ execution$

options\clbcatq.dll

Opens key: HKLM\software\microsoft\com3\debug

Opens key: HKLM\software\classes

Opens key: HKCR\clsid

Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\treatas

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\inprocserverx86

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\localserver32

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver32

Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\inprochandler32

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler32

Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\inprochandlerx86

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\localserver

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver

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

options\ieframe.dll

Opens key: HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe

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

Opens key: HKCU\software\classes\interface\{eab22ac1-30c1-11cf-a7eb-

0000c05bae0b}\typelib

 $\label{thm:continuous} Opens \ key: \\ HKCR \ interface {$eab22ac1-30c1-11cf-a7eb-0000c05bae0b} \ typelib \\ Opens \ key: \\ HKCU \ software \ classes \ clsid {$a4a1a128-768f-41e0-bf75-e4fddd701cba} \ \\ \\$

00aa00404770}\proxystubclsid32

Opens key: HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32

Opens key: HKCU\software\classes\interface\{79eac9c4-baf9-11ce-8c82-

00aa004ba90b}\proxystubclsid32

Opens key: HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32

Opens key: HKCU\software\classes\interface\{000214e6-0000-0000-c000-

00000000046}\proxystubclsid32

Opens key: HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32

Opens key: HKCU\software\classes\interface\{93f2f68c-1d1b-11d3-a30e-

00c04f79abd1}\proxystubclsid32

Opens key: HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1\}\proxystubclsid32

Opens key: HKCU\software\classes\clsid\{11016101-e366-4d22-bc06-

4ada335c892b}\shellfolder

Opens key: HKCU\software\classes\clsid\{1f4de370-d627-11d1-ba4f-

00a0c91eedba}\shellfolder

Opens key: HKCR\clsid\{1f4de370-d627-11d1-ba4f-00a0c91eedba}\shellfolder

Opens key: HKCU\software\classes\clsid\{450d8fba-ad25-11d0-98a8-

0800361b1103}\shellfolder

Opens key: HKCU\software\classes\clsid\{645ff040-5081-101b-9f08-

00aa002f954e}\shellfolder

Opens key: HKCR\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder

Opens key: HKCU\software\classes\clsid\{e17d4fc0-5564-11d1-83f2-

00a0c90dc849}\shellfolder

 $Opens~key: \\ HKCR\clsid\{e17d4fc0-5564-11d1-83f2-00a0c90dc849}\\\ \shellfolder$

Opens key:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus shell execute hooks$

HKCU\software\classes\clsid\{aeb6717e-7e19-11d0-97ee-Opens key:

00c04fd91972}\inprocserver32

Opens kev: HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32 Opens key: HKLM\software\microsoft\windows\currentversion\app paths\cmd.exe HKLM\software\microsoft\windows\currentversion\policies\associations Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\policies\associations

Opens key: HKCU\software\classes\.exe

HKCR\.exe Opens key:

Opens key: HKCU\software\classes\.ade

Opens key: HKCR\.ade

Opens key: HKCU\software\classes\.adp

Opens key: HKCR\.adp

Opens key: HKCU\software\classes\.app Opens key: HKCR\.app HKCU\software\classes\.asp Opens kev:

Opens key: HKCR\.asp

Opens key: HKCU\software\classes\.bas

Opens key: HKCR\.bas

Opens key: HKCU\software\classes\.bat

Opens key: HKCR\.bat

Opens kev: HKCU\software\classes\.cer

Opens key: HKCR\.cer

Opens key: HKCU\software\classes\.chm

Opens key: HKCR\.chm

Opens key: HKCU\software\classes\.cmd

Opens key: HKCR\.cmd

Opens key: HKCU\software\classes\.com

Opens key: HKCR\.com

Opens key: HKCU\software\classes\.cpl

Opens key: HKCR\.cpl

Opens key: HKCU\software\classes\.crt

Opens key: HKCR\.crt

HKCU\software\classes\.csh Opens key:

Opens key: HKCR\.csh

Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}

HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4} Opens key: Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\treatas

HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\inprocserver32

HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\inprocserverx86

 $HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserverx86$ Opens key: Opens key:

HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver32

HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver32 Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-Opens kev:

00c04fb6bfc4}\inprochandler32

 $HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32$ Opens key:

HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-Opens key:

00c04fb6bfc4}\inprochandlerx86

 $HKCR \c1sid \end{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4} \label{fig:hkcr} in prochandler x 86 \end{6mm}$ Opens key:

HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-Opens key:

00c04fb6bfc4}\localserver

 $HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver$ Opens key:

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610 Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610

HKCU\software\microsoft\internet Opens kev:

explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000 Opens key:

HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{20d04fe0-3aea-1069a2d8-08002b30309d}

Opens key: 08002b30309d}\inprocserver32

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

options\setupapi.dll

Opens kev: HKLM\svstem\currentcontrolset\control\minint

Opens key: HKLM\system\wpa\pnp

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

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

Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume

Opens kev:

```
11e3-9fc7-806d6172696f}\
 Opens key:
                         HKCU\software\classes\drive\shellex\folderextensions
                         HKCR\drive\shellex\folderextensions
 Opens key:
                         HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-
 Opens key:
4442-804e-409d6c4515e9}
 Opens key:
                         HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}
 Opens key:
                         HKCU\software\classes\directory
 Opens key:
                         HKCR\directory
                         HKCU\software\classes\directory\curver
 Opens key:
 Opens key:
                         HKCR\directory\curver
 Opens key:
                         HKCR\directory\
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\policies\system
                         HKCU\software\classes\directory\shellex\iconhandler
 Opens key:
 Opens key:
                         HKCR\directory\shellex\iconhandler
 Opens key:
                         HKCU\software\classes\directory\clsid
 Opens key:
                         HKCR\directory\clsid
 Opens key:
                         HKCU\software\classes\folder
 Opens key:
                         HKCR\folder
 Opens key:
                         HKCU\software\classes\folder\clsid
 Opens key:
                         HKCR\folder\clsid
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\explorer\fileexts
                         HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.exe
 Opens kev:
 Opens key:
                         HKCU\software\classes\exefile
 Opens key:
                         HKCR\exefile
                         HKCU\software\classes\exefile\curver
 Opens key:
 Opens key:
                         HKCR\exefile\curver
 Opens key:
                         HKCR\exefile\
 Opens key:
                         HKCU\software\classes\exefile\shellex\iconhandler
 Opens key:
                         HKCR\exefile\shellex\iconhandler
 Opens key:
                         HKCU\software\classes\systemfileassociations\.exe
 Opens key:
                         HKCR\systemfileassociations\.exe
 Opens key:
                         HKCU\software\classes\systemfileassociations\application
 Opens key:
                         HKCR\systemfileassociations\application
                         HKCU\software\classes\exefile\clsid
 Opens key:
 Opens key:
                         HKCR\exefile\clsid
 Opens key:
                         HKCU\software\classes\*
                         HKCR\*
 Opens key:
 Opens key:
                         HKCU\software\classes\*\clsid
 Opens key:
                         HKCR\*\clsid
                         HKCU\software\classes\exefile\shell
 Opens key:
 Opens key:
                         HKCR\exefile\shell
 Opens key:
                         HKCU\software\classes\exefile\shell\open
                         HKCR\exefile\shell\open
 Opens key:
 Opens key:
                         HKCU\software\classes\exefile\shell\open\command
 Opens key:
                         HKCR\exefile\shell\open\command
 Opens key:
HKCU\software\classes\exefile\shell\open\ddeexec
 Opens kev:
                         HKCR\exefile\shell\open\ddeexec
 Opens key:
 Opens key:
                         HKCU\software\classes\applications\cmd.exe
 Opens key:
                         HKCR\applications\cmd.exe
                         HKCU\software\microsoft\windows\shellnoroam
 Opens key:
 Opens key:
                         {\tt HKCU \backslash software \backslash microsoft \backslash windows \backslash shell no roam \backslash muicache}
 Opens kev:
                         HKCU\software\microsoft\windows\shellnoroam\muicache\
 Opens key:
                         HKLM\system\currentcontrolset\control\session manager\appcertdlls
 Opens key:
                         HKLM\system\wpa\tabletpc
 Opens key:
                         HKLM\system\wpa\mediacenter
                         HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
 Opens kev:
 Opens key:
                         HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\cmd.exe
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\appcompatflags
 Opens key:
                         HKCU\software\microsoft\windows nt\currentversion\appcompatflags
 Opens key:
                         HKLM\software\policies\microsoft\windows\safer\levelobjects
 Opens key:
                         HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
 Opens key:
be2efd2c1a33}
 Opens key:
                         HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes
```

Opens key:

edd5fbde1328}

Opens kev:

b813f72dbb91}

Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-

7c29ddecae3f} Opens kev:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes \setminus \{94e3e076-8f53-42a5-8411-4264-8411-4264-8411-4264-8411-4264-8411-4264-8411-4264-8411-4264-8411-4264-841$

085bcc18a68d} Opens kev:

```
b91490411bfc}
 Opens kev:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
  Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
  Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus urlzones
                              HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
  Opens key:
                             HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
  Opens key:
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
  Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus paths
  Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus has hes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
  Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
  Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus urlzones
  Opens key:
                             HKCU\software\microsoft\windows\currentversion\explorer\shell folders
                              HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\cmd.exe
  Opens key:
                              HKLM\software\microsoft\windows
  Opens key:
                              HKLM\software\microsoft\windows\html help
  Opens key:
                              HKLM\software\microsoft\windows\help
  Opens key:
                              \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\acgenral.dll
                              HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens kev:
options\shimeng.dll
  Opens key:
                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msacm32.dll
 Opens key:
                              \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution
options\uxtheme.dll
                              HKLM\software\microsoft\audiocompressionmanager\drivercache
  Opens kev:
  Opens key:
```

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm

Opens kev:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm

Opens key: $HKLM \ \ software \ \ microsoft \ \ audio compression manager \ \ \ driver cache \ \ msg711$

Opens kev:

 $HKLM \ software \ microsoft\ audio compression manager \ driver cache \ msacm. msgsm610$

Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723 Opens kev:

Opens key:

 $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. \ msaudio 1$

Opens kev:

 $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. sl_anet$

Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2 Opens key: Opens kev: HKLM\system\currentcontrolset\control\mediaresources\acm HKCU\software\microsoft\windows\currentversion\thememanager Opens key: Opens key: HKCU\software\policies\microsoft\windows\system Opens key: HKLM\software\microsoft\command processor Opens key: HKCU\software\microsoft\command processor Opens key: HKLM\system\currentcontrolset\control\nls\locale Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts Opens key: HKLM\system\currentcontrolset\control\nls\language groups Opens kev: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\tasklist.exe Opens key: $\label{lem:hklmsoftware} \mbox{\tt HKLM} \mbox{\tt software} \mbox{\tt microsoft} \mbox{\tt windows nt} \mbox{\tt current} \mbox{\tt version} \mbox{\tt image file execution}$ options\tasklist.exe Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mpr.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\framedyn.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dbghelp.dll Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder Opens key: HKLM\software\microsoft\wbem\cimom Opens kev: HKLM\software\microsoft\ctf\compatibility\tasklist.exe Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\tasklist.exe\rpcthreadpoolthrottle HKLM\system\currentcontrolset\control\lsa Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\xpsp2res.dll HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24} Opens key: Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24} Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\treatas Opens key: $HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\$ \treatas Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32 Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32 Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserverx86 HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserverx86 Opens key: Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\localserver32 HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\localserver32 Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-Opens kev: 00aa004b2e24}\inprochandler32 HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler32 Opens kev: Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandlerx86 Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandlerx86 Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\localserver HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\localserver Opens key:

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

options\wbemcomn.dll

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

options\wbemprox.dll

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

options\winsta.dll

Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}

HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820} Opens key: Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\treatas

Opens key: $HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820\}\treatas$ Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprocserver32

 $HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820\}\inprocserver32$ Opens key:

Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprocserverx86

Opens key:

Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\localserver32

HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprochandler32

 $HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820\}\inprochandler 32$ Opens key:

Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprochandlerx86

Opens key:

HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-Opens key:

00c04fb68820}\localserver

HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus appid \setminus \{8bc3f05e-d86b-11d0-a075-00c04fb68820\}$

HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820} Opens key:

Opens key: $HKCU \setminus software \setminus classes \setminus interface \setminus \{f309ad18 - d86a - 11d0 - a075 - 00c04fb68820\}$ Opens key: HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}
Opens key: HKCU\software\classes\interface\{f309ad18-d86a-11d0-a075-

00c04fb68820}\proxystubclsid32

Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-

00aa004b2e24}\treatas

00aa004b2e24}\inprocserver32

Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32

Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-

00aa004b2e24}\inprocserverx86

Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-

00aa004b2e24}\localserver32

Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\localserver32

Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-

00aa004b2e24}\inprochandler32

Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler32

Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-

00aa004b2e24}\inprochandlerx86

Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-

00aa004b2e24}\localserver

Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\localserver

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

options\wbemsvc.dll

Opens key: HKCU\software\classes\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}

Opens key: HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}
Opens key: HKCU\software\classes\interface\{d4781cd6-e5d3-44df-ad94-

930efe48a887}\proxystubclsid32

Opens key: HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32
Opens key: HKCU\software\classes\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}

Opens key: HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}
Opens key: HKCU\software\classes\interface\{9556dc99-828c-11cf-a37e-

00aa003240c7}\proxystubclsid32

Opens key: $\label{eq:hccn} \begin{tabular}{ll} HKCR\interface \ 9556dc99-828c-11cf-a37e-00aa003240c7\ proxystubclsid32 \\ Opens key: \\ HKCU\software \ classes \ clsid \ d68af00a-29cb-43fa-8504-ce99a996d9ea \ \end{tabular}$

Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\treatas

 Opens key:
 HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\treatas

 Opens key:
 HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504

ce99a996d9ea}\inprocserver32

Opens key: $\label{eq:hkcr} \mbox{HKCR\clsid\d68af00a-29cb-43fa-8504-ce99a996d9ea} \mbox{\label{eq:hkcr} inprocserver32}$

Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\inprocserverx86

Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserverx86

Opens key: $\label{local-continuous} \mbox{HKCU\software\classes\clsid\d68af00a-29cb-43fa-8504-} \\$

ce99a996d9ea}\localserver32

 $Opens~key: \\ HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\ \ localserver 32$

Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\inprochandler32

Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandler32

Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-

 $ce 99a 996d 9ea \} \verb|\inprochandlerx86|$

Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\localserver

Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\localserver

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

options\msvcp60.dll

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

options\wldap32.dll

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

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

options\ntdsapi.dll

Opens key: $\label{thm:limit} \mbox{HKLM} software \mbox{\sc microsoft} \mbox{\sc microsoft}$

Opens key: HKCU\software\classes\interface\{027947e1-d731-11ce-a357-000000000001} Opens key: HKCR\interface\{027947e1-d731-11ce-a357-00000000001}

Opens key: HKCU\software\classes\interface\{027947e1-d731-11ce-a357-00000000001}\proxystubclsid32

Opens key: HKCR\interface\{027947e1-d731-11ce-a357-00000000001}\proxystubclsid32
Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}

 Opens key:
 HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}

 Opens key:
 HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604

00104b703efd}\treatas

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\treatas Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

 $00104b703efd \verb|\inprocserver32|$

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32

Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprocserverx86

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\localserver32

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\localserver32

Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprochandler32

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler32

Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprochandlerx86

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\localserver

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\localserver

Opens key: HKCU\software\classes\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}

Opens key: HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd\}
Opens key: HKCU\software\classes\interface\{1c1c45ee-4395-11d2-b60b-

00104b703efd}\proxystubclsid32

 $\label{lem:continuous} Opens key: $$ HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd} \rightarrow HKCU\software\classes\interface\{423ec01e-2e35-11d2-b604-00104b703efd} $$$

Opens key: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}
Opens key: HKCU\software\classes\interface\{423ec01e-2e35-11d2-b604-

00104b703efd}\proxystubclsid32

Opens key: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat] Queries value:

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

Queries value: HKLM\system\currentcontrol\session manager[safedllsearchmode]

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

nt\currentversion\compatibility32[709ce21bcb87f234c01594e44f12936e]

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

compatibility[709ce21bcb87f234c01594e44f12936e]

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

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

manager[criticalsectiontimeout]

Queries value: HKLM\software\microsoft\ole[rwlockresourcetimeout]
Queries value: HKCR\interface[interfacehelperdisableall]

Queries value: HKCR\interface[interfacehelperdisableallforole32]
Queries value: HKCR\interface[interfacehelperdisabletypelib]

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

00000000046}[interfacehelperdisableall]

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

00000000046}[interfacehelperdisableallforole32]

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

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

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

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

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

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

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

manager[safeprocesssearchmode]

Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
Queries value: HKCU\software\microsoft\ctf[disable thread input manager]
Queries value: HKLM\system\currentcontrol\set\control\nls\codepage[932]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[949]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[950]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[936]
Queries value: HKLM\system\currentcontrolset\services\disk\enum[0]

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

Queries value:

 $\label{lem:hkcusoftware} HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips] \\ Queries\ value: HKLM\software\microsoft\windows\currentversion\internet \\$

settings[disableimprovedzonecheck]

 $\label{thm:linear} \textit{Queries value:} \qquad \qquad \textit{HKLM} \\ \textit{software} \\ \textit{microsoft} \\ \textit{internet}$

 $explorer \verb|\main| feature_protocol_lockdown[709ce21bcb87f234c01594e44f12936e.exe]|$

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

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

ab78-1084642581fb]

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

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

settings[fromcachetimeout]

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

settings[secureprotocols]

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

explorer\main[security_hklm_only]

```
Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[disablepassport]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[enablehttp1_1]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[proxyhttp1.1]
  Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
settings[enablenegotiate]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[disablebasicoverclearchannel]
                           HKCU\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol[feature clientauthcertfilter]
                           HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[syncmode5]
                           HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache[signature]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\content[peruseritem]
                           HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\content[peruseritem]
  Queries value:
                           HKLM\system\setup[systemsetupinprogress]
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Queries value:
folders[cache]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\content[cachelimit]
                           \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{$microsoft$} \windows \current version \end{tabular} internet \\ \end{tabular}
  Queries value:
settings\5.0\cache\cookies[peruseritem]
  Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Queries value:
folders[cookies]
                           \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
  Queries value:
settings\5.0\cache\cookies[cacheprefix]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cachelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\history[peruseritem]
  Queries value:
                           \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
settings\5.0\cache\history[peruseritem]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
  Queries value:
                           HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
HKLM\svstem\currentcontrolset\computername\activecomputername[computername]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacherepair]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cachepath]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheprefix]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cacheoptions]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacherepair]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
  Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
```

```
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
                              HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacherepair]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachepath]
                              \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\extensible cache\iecompat[cacheprefix]
                              \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
  Oueries value:
settings\5.0\cache\extensible cache\iecompat[cachelimit]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
                              \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\extensible cache\ietld[cacherepair]
                             HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\ietld[cachepath]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\ietld[cacheprefix]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\ietld[cachelimit]
                              \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\extensible cache\ietld[cacheoptions]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
                              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\privacie:[cacherepair]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
  Queries value:
                              \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\extensible cache\privacie:[cachelimit]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
                              \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
  Oueries value:
settings[disableworkerthreadhibernation]
  Queries value:
                              \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
settings[disableworkerthreadhibernation]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
                              HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[socketsendbufferlength]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[socketreceivebufferlength]
  Queries 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
  Oueries value:
settings[maxconnectionsperserver]
  Queries value:
                              HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
                              HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[maxconnectionsper1_0server]
  Oueries value:
                              HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1 Oserver]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
                              HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[serverinfotimeout]
  Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value:
                              HKLM\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
                              HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[connectretries]
```

```
Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[connectretries]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendtimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[receivetimeout]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablentlmpreauth]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[scavengecachelowerbound]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[certcachenovalidate]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelifetime]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[ftpdefaultexpirytimesecs]
                           HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[709ce21bcb87f234c01594e44f12936e.exe]
 Oueries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablecachingofsslpages]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[perusercookies]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[leashlegacycookies]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablent4rascheck]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dialupuselansettings]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendextracrlf]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[bypassftptimecheck]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduringauth]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[releasesocketduring401auth]
                           \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
 Oueries value:
settings[releasesocketduring401auth]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablelegacypreauthasserver]
 Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasshttpnocachecheck]
 Queries value:
                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[bvpasssslnocachecheck]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[enablehttptrace]
 Queries value:
                           \label{lem:hkcu} \verb+KCU\+software\+microsoft\+windows\+currentversion\+internet
settings[nocheckautodialoverride]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dontusednsloadbalancing]
 Queries value:
                           \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
settings[dontusednsloadbalancing]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[mimeexclusionlistforcache]
 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[headerexclusionlistforcache]
```

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

Queries value:

```
settings[dnscacheenabled]
                                                    HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[dnscacheentries]
   Queries value:
                                                    HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
   Queries value:
                                                    HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
   Oueries value:
                                                    HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
   Queries value:
                                                    HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
   Queries value:
                                                    \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
settings[warnonbadcertsending]
   Queries value:
                                                   HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
                                                    HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[warnonpostredirect]
   Queries value:
                                                   HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
                                                   HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[warnonhttpstohttpredirect]
   Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters [winsock_registry_version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
   Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 [next\_catalog\_entry\_id]
   Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ (0000000000002 [packed catalog item]) \ details \ 
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000005[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\00000000007[packedcatalogitem]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ (000000000008 [packed catalog item]) \ details \ d
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
   Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 000000000011 \ [packed catalog item]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
   Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace \_catalog5 \ catalog\_entries \ 00000000001 [library path]
   Oueries value:
Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ (catalog\_entries \ 000000000001 \ [address family]
   Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000001[supported name space]
Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000002[librarypath]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ (catalog\_entries \ 0000000000002 \ [displaystring]
   Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ name space\_catalog \ na
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
   Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 00000000000002[supported name space]]
   Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog 5 \setminus catalog\_entries \setminus 00000000000002 [enabled]
```

Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 00000000000002 \ [version]$

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\000000000003[librarypath]
 Oueries value:

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
Queries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
Queries value:

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

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 000000000003 [storesservice class info] \ Queries \ value:$

 $\label{local-equation} HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws 2_32 numhandle buckets]$

Queries value:

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]

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

settings[globaluseroffline]

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

settings[enableautodial]
Oueries value:

 $\label{thm:linear} Queries \ value: \\ HKLM\software\microsoft\windows\currentversion\internet$

settings[urlencoding]
Oueries value:

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

settings[truncatefilename]

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

settings[badproxyexpirestime]

HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3] HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6] HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7] Queries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi] Oueries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1] Oueries value: $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [midi2]$ Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6] Oueries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]

Queries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]

Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer] Oueries value: $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [mixer 1]$ Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer31 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]

Queries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus telephony [tapi32 max numre questre tries]$

Queries value:

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

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

folders[common appdata]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\winlogon[userenvdebuglevel]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\winlogon[chkaccdebuglevel]

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

folders[personal]

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

folders[local settings]

HKLM\software\microsoft\windows Queries value:

nt\currentversion\winlogon[rsopdebuglevel]

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

HKLM\software\microsoft\windows Queries value: nt\currentversion\profilelist[profilesdirectory]

HKLM\software\microsoft\windows Queries value:

nt\currentversion\profilelist[allusersprofile]

HKLM\software\microsoft\windows Oueries value: nt\currentversion\profilelist[defaultuserprofile]

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

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

nt\currentversion\winlogon[parseautoexec]

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

folders[appdata]

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

settings[migrateproxy]

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

settings[proxyenable]

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

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

settings\connections[savedlegacysettings]

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

settings\connections[defaultconnectionsettings]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_mime_handling[709ce21bcb87f234c01594e44f12936e.exe]

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

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

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

explorer\security[disablesecuritysettingscheck]

Queries value: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}$

settings\zones\0[flags] Oueries value:

HKCU\software\microsoft\windows\currentversion\internet

settings\zones\1[flags]

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

settings\zones\2[flags]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[flags]

Oueries value:

HKCU\software\microsoft\windows\currentversion\internet

settings\zones\4[flags]

HKCU\software\microsoft\internet Oueries value:

explorer\main\featurecontrol\feature_localmachine_lockdown[709ce21bcb87f234c01594e44f12936e.exe]

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

explorer\main\featurecontrol\feature_localmachine_lockdown[709ce21bcb87f234c01594e44f12936e.exe]

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

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

settings[createuricachesize]

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

settings[createuricachesize]

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

settings[enablepunycode]

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

settings[enablepunycode]

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

settings\zonemap[autodetect]

Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1a10] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [prioritize record data]$ Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [register primary name]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Oueries value: Queries value: Queries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile] Queries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [multicastlisten level]$

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts] Oueries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]

Oueries value:

c7d49d7cecdc}[enabledhcp]

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-4404, and an armonic set \ services \ tcpip \ parameters \ interfaces \ tcpip \ parameters \ terrange \ tcpip \ parameters \ tcpip \ parameters$ c7d49d7cecdc}[leaseobtainedtime]

Oueries value:

c7d49d7cecdc}[leaseterminatestime]

Oueries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-4404, and an armonic set \ services \ tcpip \ parameters \ interfaces \ tcpip \ parameters \ terrange \ tcpip \ parameters \ tcpip \ parameters$ c7d49d7cecdc}[dhcpserver]

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

c7d49d7cecdc}[queryadaptername]

Queries value:

c7d49d7cecdc}[disableadapterdomainname]

Queries value:

c7d49d7cecdc}[registrationenabled]

Queries value:

c7d49d7cecdc}[registeradaptername]

Queries value:

c7d49d7cecdc}[registrationmaxaddresscount]

c7d49d7cecdc}[maxnumberofaddressestoregister]

c7d49d7cecdc}[domain]

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4303-abe3-4304-a$ c7d49d7cecdc}[dhcpdomain]

c7d49d7cecdc}[ipautoconfigurationenabled]

c7d49d7cecdc}[addresstype]

Queries value:

c7d49d7cecdc}[nameserver]

Oueries value:

c7d49d7cecdc}[dhcpnameserver]

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

Queries value:

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

 $HKLM \ software \ microsoft \ strong$ Queries value: cryptographic provider[type]

HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong Queries value: cryptographic provider[image path]

HKLM\software\microsoft\rpc\securityservice[10] Queries value:

Oueries value:

HKLM\system\currentcontrolset\control\securityproviders[securityproviders] HKLM\software\microsoft\cryptography[machineguid] Oueries value:

 $HKLM \verb|\system| current control \verb|\sa| sspicache \verb|\msapsspc.dll[name]|$ Queries value: Oueries value:

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

Queries value:

HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]

HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid] Oueries value:

Queries value:

HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[version]

Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]

Oueries value:

HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]

HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name] Oueries value: Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]

Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities] Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version] Queries value: Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize] HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name] Oueries value: Oueries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel] HKLM\system\currentcontrolset\services\winsock\parameters[transports] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities] HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid] Oueries value: Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type] Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname] HKLM\system\currentcontrolset\services\netbt\linkage[export] Queries value: HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps] Oueries value: Queries value: HKLM\software\microsoft\windows\currentversion\explorer[maximizeapps] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nonethood] HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups] bc06-4ada335c892b}[suppressionpolicy] ba4f-00a0c91eedba}[suppressionpolicy] 98a8-0800361b1103}[suppressionpolicy] $HKLM \setminus software \setminus irrosoft \setminus ir$ 9f08-00aa002f954e}[suppressionpolicy] Oueries value: $HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{e17d4fc0-5564-11d1-e17d4fc0-55646-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-55$ 83f2-00a0c90dc849}[suppressionpolicy] HKCR\clsid\{20d04fe0-3aea-1069-a2d8-Queries value: 08002b30309d}\shellfolder[wantsparsedisplayname] Queries value: HKCR\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder[wantsparsedisplayname] Oueries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-

 $08002b30309d \verb|\shellfolder[wantsparsedisplayname]|$

Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[]

Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\inprocserver32[loadwithoutcom]

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

 $extensions \verb|\blocked| \{871c5380-42a0-1069-a2ea-08002b30309d\}|$

 $\label{thm:current} Queries \ value: \\ HKCU \ software \ microsoft \ windows \ current version \ shell \\$

extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]

Queries value:

 $\label{prop:linear_lambda} HKCU \software \mbox{\tt microsoft} \windows \current version \policies \explorer [enforces hellex tension security]$

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

extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}

0x401]

Queries value: HKCU\software\microsoft\windows\currentversion\shell extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-00000000046}

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

manager\appcompatibility[disableappcompat]

Queries value: HKLM\software\microsoft\com3[com+enabled]

Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]

Queries value: HKLM\software\microsoft\com3[regdbversion] Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[appid]

```
HKCR\clsid\{871c5380-42a0-1069-a2ea-
  Oueries value:
08002b30309d}\inprocserver32[threadingmodel]
  Oueries value:
                                    HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe[]
  Queries value:
                                    HKLM\software\microsoft\internet explorer\setup[iexplorelastmodifiedlow]
                                    HKLM\software\microsoft\internet
  Oueries value:
explorer\setup[iexplorelastmodifiedhigh]
                                    HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib[]
  Oueries value:
  Oueries value:
                                    HKLM\software\microsoft\internet explorer\setup[installstarted]
  Oueries value:
                                    HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32[]
  Oueries value:
                                    HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32[]
                                    HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32[]
  Oueries value:
  Queries value:
                                    HKCR \ interface \ \{93f2f68c-1d1b-11d3-a30e-00c04f79abd1\} \ proxystubclsid32[]
  Queries value:
                                    HKCR\clsid\{11016101-e366-4d22-bc06-
4ada335c892b}\shellfolder[wantsparsedisplayname]
                                    HKCR\clsid\{1f4de370-d627-11d1-ba4f-
  Queries value:
00a0c91eedba}\shellfolder[wantsparsedisplayname]
                                    HKCR\clsid\{450d8fba-ad25-11d0-98a8-
  Oueries value:
0800361b1103}\shellfolder[wantsparsedisplayname]
  Queries value:
                                    HKCR\clsid\{645ff040-5081-101b-9f08-
00aa002f954e}\shellfolder[wantsparsedisplayname]
                                    HKCR\clsid\{e17d4fc0-5564-11d1-83f2-
  Queries value:
00a0c90dc849}\shellfolder[wantsparsedisplayname]
                                    HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32[]
  Oueries value:
                                    HKCR\clsid\{aeb6717e-7e19-11d0-97ee-
  Queries value:
00c04fd91972}\inprocserver32[loadwithoutcom]
                                    HKCR\.exe[]
  Queries value:
  Queries value:
                                    HKCR\.asp[]
  Queries value:
                                    HKCR\.bat[]
                                    HKCR\.cer[]
  Oueries value:
                                    HKCR\.chm[]
  Queries value:
                                    HKCR\.cmd[]
  Oueries value:
  Queries value:
                                    HKCR\.com[]
                                    HKCR\.cpl[]
  Queries value:
  Queries value:
                                    HKCR\.crt[]
                                    HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
  Oueries value:
00c04fb6bfc4}\inprocserver32[inprocserver32]
                                    HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[]
  Oueries value:
                                    HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[appid]
  Oueries value:
                                    HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
  Queries value:
00c04fb6bfc4}\inprocserver32[threadingmodel]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
                                    HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[specialfolderscachesize]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1806]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[]
  Oueries value:
  Oueries value:
                                    HKLM\system\wpa\pnp[seed]
  Queries value:
                                    HKLM\system\setup[osloaderpath]
  Queries value:
                                    HKLM\system\setup[systempartition]
                                    HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
  Oueries value:
  Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]
                                    HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
  Queries value:
  Queries value:
                                    HKLM\software\microsoft\windows\currentversion[devicepath]
  Oueries value:
                                    HKLM\software\microsoft\windows\currentversion\setup[loglevel]
                                    HKLM\software\microsoft\windows\currentversion\setup[logpath]
  Queries value:
  Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints 2 \ cpc \ volume \ \{f90255c2-6bc4-f9025fc2-f9bc4-f9025fc2-f9bc4-f9025fc2-f9bc4-f9025fc2-f9bc4-f9025fc2-f9bc4-f9025fc2-f9bc4-f9025fc2-f9bc4-f9025fc2-f9bc4-f9025fc2-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-f9bc4-
11e3-9fc7-806d6172696f}[data]
  Queries value:
11e3-9fc7-806d6172696f}[generation]
                                    HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
  Oueries value:
409d6c4515e9}[drivemask]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]
HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell]
  Queries value:
```

```
HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
                                                  \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{tabular} hidden \cite{tabular} \end{tabular}
   Queries value:
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
   Oueries value:
Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
                                                  HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
   Queries value:
HKCR\directory[docobject]
   Queries value:
   Oueries value:
                                                  HKCR\directory[browseinplace]
                                                  HKCR\directory[isshortcut]
   Queries value:
   Queries value:
                                                  HKCR\directory[alwaysshowext]
   Queries value:
                                                  HKCR\directory[nevershowext]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]
                                                  HKCR\exefile[docobiect]
   Oueries value:
                                                  HKCR\exefile[browseinplace]
   Queries value:
                                                  HKCR\exefile[isshortcut]
   Oueries value:
   Oueries value:
                                                  HKCR\exefile[alwaysshowext]
                                                  HKCR\exefile[nevershowext]
   Queries value:
                                                  HKCR\exefile\shell[]
   Queries value:
   Queries value:
                                                  HKCR\exefile\shell\open\command[]
                                                  HKCR\exefile\shell\open\command[command]
   Queries value:
   Oueries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[flags]
   Oueries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[state]
   Queries value:
                                                  HKLM \  \  \, nt\  \  \, \
1757981266-507921405-1957994488-1003[userpreference]
                                                 HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
   Oueries value:
1757981266-507921405-1957994488-1003[centralprofile]
                                                  HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
   Oueries value:
1757981266-507921405-1957994488-1003[profileloadtimelow]
   Queries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[profileloadtimehigh]
                                                 HKCU\software\microsoft\windows\shellnoroam\muicache[langid]
   Oueries value:
   Queries value:
HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\cmd.exe]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[inheritconsolehandles]
HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[disallowrun]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[norunasinstallprompt]
                                                  HKLM\system\wpa\mediacenter[installed]
   Queries value:
HKLM \verb| software \verb| policies \verb| microsoft \verb| windows \verb| safer \verb| code identifiers [authenticode enabled] |
   Queries value:
                                                  HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
   Oueries value:
be2efd2c1a33}[itemdata]
   Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}[saferflags]
   Oueries value:
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ has hes \ \{349d35ab-37b5-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-46666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b
edd5fbde1328}[itemdata]
   Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[hashalg]
   Oueries value:
```

```
edd5fbde1328}[itemsize]
Queries value:
HKLM\software\policies\mi
edd5fbde1328}[saferflags]
```

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-

Oueries value:

 $\label{thm:local_ham} $HKLM\software policies \microsoft\windows \afer\code identifiers \oldsymbol{hashes} \{7fb9cd2e-3076-4df9-a57b-b813f72dbb91\}[itemdata] }$

Oueries value:

Oueries value:

Oueries value:

Queries value:

Queries value:

Oueries value:

Queries value:

Oueries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{94e3e076-8f53-42a5-8411-085bcc18a68d\} \ fitem \ data \ for the policies \ microsoft \ hashes \ has$

Queries value:

 $\label{thm:local-bound} HKLM software \policies \microsoft \windows \safer \code identifiers \0 \hashes \94e3e076-8f53-42a5-8411-085bcc18a68d \[hashalg \]$

Oueries value:

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

Queries value:

 $HKLM \ software \ blicies \ icrosoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{94e3e076-8f53-42a5-8411-085bcc18a68d\} [saferflags]$

Queries value:

 $HKLM \ software \ b01490411bfc} iiers \ 0\ hashes \ dc971ee5-44eb-4fe4-ae2e-b91490411bfc} iiers \ b01490411bfc \ iierdata \ b01490411bfc \ iierdata \ b01490411bfc \ iierdata \ iierdata$

Queries value:

 $HKLM \ software \ b01icies \ icrosoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-b91490411bfc\} \ [hashalg]$

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-b91490411bfc\} [itemsize]$

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-b91490411bfc\} \ [saferflags]$

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]

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

folders[cache]
 Queries value:

 $\label{thm:loss} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} policies \end{tabular} irror soft \end{tabular} windows \end{tabular} software \end{tabular} policies \end{tabular} irror soft \end{tabular} windows \end{tabular} software \end{tabular} policies \end{tabular} metalor software \end{tabular} windows \end{tabular} windows \end{tabular} software \end{tabular} windows \end{tabular} windows \end{tabular} windows \end{tabular} windows \end{tabular} software \end{tabular} windows \end{t$

 Queries value:
 HKCU\software\microsoft\visual basic\6.0[allowunsafeobjectpassing]

 Queries value:
 HKLM\software\microsoft\windows nt\currentversion\compatibility32[cmd]

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

Queries value: HKLM\software\microsoft\windows

nt\currentversion\drivers32[msacm.imaadpcm]

Queries value:

Queries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags]

Queries value:

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

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cfiltertags]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\drivers32[msacm.msadpcm]

Queries value:

Queries value:

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

Queries value:

 $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msadpcm[aformattag cache]$

Queries value

```
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cfiltertags]
                          HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\drivers32[msacm.msg711]
 Queries value:
HKLM \verb|\software\microsoft\audiocompressionmanager\drivercache\mbox| msg711[fdwsupport]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cformattags]
 Oueries value:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msg711[aformattag cache]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cfiltertags]
                          HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\drivers32[msacm.msgsm610]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[fdwsupport]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cformattags]
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msgsm610 [a formattag cache]
 Queries value:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. msgsm610[cfilter tags]
                          HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\drivers32[msacm.trspch]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport]
 Queries value:
HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus msacm.trspch[cformattags]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cfiltertags]
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msg723]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[fdwsupport]
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cformattags]
 Queries value:
HKLM \backslash software \backslash microsoft \backslash audio compression manager \backslash driver cache \backslash msacm. msg723 [aformattag cache]
 Queries value:
HKLM \verb|\software\microsoft\audiocompressionmanager\drivercache\mbox{|} msg723[cfiltertags]|
                          HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msaudio1]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[fdwsupport]
 Queries value:
HKLM \verb| software \verb| microsoft \verb| audiocompression manager \verb| driver cache \verb| msaudio1[cformattags]| \\
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[aformattagcache]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cfiltertags]
                          HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\drivers32[msacm.sl_anet]
 Queries value:
HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus msacm. sl\_anet[fdwsupport]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cformattags]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[aformattagcache]
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl anet[cfiltertags]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2\fdwsupport1
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cformattags]
 Queries value:
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cfiltertags]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.l3acm]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[fdwsupport]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cformattags]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[aformattagcache]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags]
                          HKCU\software\microsoft\multimedia\audio compression
 Oueries value:
manager\msacm[nopcmconverter]
                          HKCU\software\microsoft\multimedia\audio compression manager\priority
 Oueries value:
v4.00[priority1]
```

```
Oueries value:
                          HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
 Oueries value:
                          HKCU\control panel\desktop[lamebuttontext]
                          HKLM\software\microsoft\command processor[disableunccheck]
 Oueries value:
 Queries value:
                          HKLM\software\microsoft\command processor[enableextensions]
 Oueries value:
                          HKLM\software\microsoft\command processor[delayedexpansion]
 Queries value:
                          HKLM\software\microsoft\command processor[defaultcolor]
                          HKLM\software\microsoft\command processor[completionchar]
 Oueries value:
                          HKLM\software\microsoft\command processor[pathcompletionchar]
 Oueries value:
 Oueries value:
                          HKLM\software\microsoft\command processor[autorun]
                          HKCU\software\microsoft\command processor[disableunccheck]
 Oueries value:
 Oueries value:
                          HKCU\software\microsoft\command processor[enableextensions]
 Queries value:
                          HKCU\software\microsoft\command processor[delayedexpansion]
 Oueries value:
                          HKCU\software\microsoft\command processor[defaultcolor]
 Oueries value:
                          HKCU\software\microsoft\command processor[completionchar]
 Oueries value:
                          HKCU\software\microsoft\command processor[pathcompletionchar]
 Queries value:
                          HKCU\software\microsoft\command processor[autorun]
                          HKLM \ system \ current controls et \ control \ nls \ locale [00000409]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\control\nls\language groups[1]
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\compatibility32[tasklist]
                          HKLM\software\microsoft\windows nt\currentversion\ime
 Queries value:
compatibility[tasklist]
                          HKLM\software\microsoft\wbem\cimom[logging]
 Oueries value:
 Queries value:
                          HKLM\software\microsoft\wbem\cimom[logging directory]
 Queries value:
                          HKLM\software\microsoft\wbem\cimom[log file max size]
 Queries value:
                          HKLM\software\microsoft\ole[maximumallowedallocationsize]
 Queries value:
                          HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
 Queries value:
                          HKCR\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[inprocserver32]
 Queries value:
                          HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32[]
 Queries value:
                          HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[appid]
                          HKCR\clsid\{4590f811-1d3a-11d0-891f-
 Queries value:
00aa004b2e24}\inprocserver32[threadingmodel]
 Queries value:
                          HKLM\software\microsoft\wbem\cimom[repository directory]
                          HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[appid]
 Oueries value:
 Queries value:
                          HKCR \land appid \land \{8bc3f05e-d86b-11d0-a075-00c04fb68820\} [dllsurrogate]
 Queries value:
                          HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[localservice]
                          HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32[]
 Oueries value:
                          HKCR\clsid\{7c857801-7381-11cf-884d-
 Queries value:
00aa004b2e24}\inprocserver32[inprocserver32]
                          HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[]
 Oueries value:
 Queries value:
                          HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[appid]
 Queries value:
                          HKCR\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[threadingmodel]
                          HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32[]
 Oueries value:
 Queries value:
                          HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32[]
 Oueries value:
                          HKCR\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[inprocserver32]
                          HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32[]
 Oueries value:
                          HKCR \verb|\clsid|{d68af00a-29cb-43fa-8504-ce99a996d9ea}[appid]
 Oueries value:
                          HKCR\clsid\{d68af00a-29cb-43fa-8504-
 Oueries value:
ce99a996d9ea}\inprocserver32[threadingmodel]
                          HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
 Oueries value:
                          HKLM\software\microsoft\wbem\cimom[processid]
 Queries value:
 Oueries value:
                          HKLM\software\microsoft\wbem\cimom[enableprivateobjectheap]
 Queries value:
                          HKLM\software\microsoft\wbem\cimom[contextlimit]
                          HKLM\software\microsoft\wbem\cimom[objectlimit]
 Oueries value:
                          HKLM\software\microsoft\wbem\cimom[identifierlimit]
 Oueries value:
                          HKCR\interface\{027947e1-d731-11ce-a357-00000000001}\proxystubclsid32[]
 Oueries value:
                          HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
 Queries value:
00104b703efd}\inprocserver32[inprocserver32]
                          HKCR \clsid \ \{1b1cad8c-2dab-11d2-b604-00104b703efd\} \ \ inprocserver 32[]
 Oueries value:
 Queries value:
                          HKCR \clsid \ \{1b1cad8c-2dab-11d2-b604-00104b703efd\} [appid]
 Queries value:
                          HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[threadingmodel]
                          HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}\proxystubclsid32[]
 Oueries value:
 Queries value:
                          HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32[]
 Value changes:
                          HKLM\software\microsoft\cryptography\rng[seed]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cookies]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[history]
 Value changes:
                          \label{lem:hklm} \verb+Kklm\+ software\+ icrosoft\+ windows\+ current version\+ explorer\+ shell
folders[common appdata]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[appdata]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
 Value changes:
                          \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings\connections[savedlegacysettings]
 Value changes:
                          \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
```

settings\zonemap[proxybypass]

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

settings\zonemap[intranetname]

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

settings\zonemap[uncasintranet]

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

settings\zonemap[autodetect]

Value changes:

806d6172696f}[baseclass]