Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3326, Task ID: 812

Task ID: 812 Risk Level: 10

Date Processed: 2016-05-18 10:41:03 (UTC)

Processing Time: 9.0 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\6f21fb21650da014d87426fa0bd8e7f2.exe"

Sample ID: 3326 Type: basic Owner: admin

Label: 6f21fb21650da014d87426fa0bd8e7f2

Date Added: 2016-05-18 10:30:51 (UTC)

File Type: PE32:win32:gui File Size: 177664 bytes

MD5: 6f21fb21650da014d87426fa0bd8e7f2

SHA256: 34f1a3cc2318939b243bfc434f9ecfa721574ded9a3958a970d0b817d536885f

Description: None

Pattern Matching Results

6 Checks task list from command line

10 Creates malicious events: Beebone [Trojan]

3 Long sleep detected

4 Terminates process under Windows subfolder

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

Creates process: C:\WINDOWS\Temp\6f21fb21650da014d87426fa0bd8e7f2.exe

["c:\windows\temp\6f21fb21650da014d87426fa0bd8e7f2.exe"]

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

tasklist&&del 6f21fb21650da014d87426fa0bd8e7f2.exe]

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

Loads service: RASMAN [C:\WINDOWS\system32\svchost.exe -k netsvcs]
Terminates process: C:\WINDOWS\Temp\6f21fb21650da014d87426fa0bd8e7f2.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

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

1957994488-1003

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

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-5079214051957994488-1003

Creates mutex: \BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-

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

settings!temporary internet files!content.ie5!

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

settings!history!history.ie5!

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

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

Creates mutex: \BaseNamedObjects\SHIMLIB_LOG_MUTEX

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

Creates semaphore: \BaseNamedObjects\C:?WINDOWS?TEMP?6F21FB21650DA014D87426FA0BD8E7F2.EXE
Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}
Creates semaphore: \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}

File System Events

Opens: C:\WINDOWS\Prefetch\6F21FB21650DA014D87426FA0BD8E-130ADCA8.pf

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

```
C:\WINDOWS\system32\rpcss.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\MSCTF.dll
                         C:\WINDOWS\system32\sxs.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\MSCTFIME.IME
 Opens:
                         C:\WINDOWS\system32\clbcatq.dll
 Opens:
                         C:\WINDOWS\system32\comres.dll
                         C:\WINDOWS\Registration\R00000000007.clb
 Opens:
 Opens:
                         C:\WINDOWS\Fonts\sserife.fon
                         C: \verb|WINDOWS\Temp\6f21fb21650da014d87426fa0bd8e7f2.exe|\\
 Opens:
 Opens:
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Config
 Opens:
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
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
 Opens:
                         C:\WINDOWS\system32\wininet.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\wininet.dll.123.Config
 Opens:
                         C:\WINDOWS\system32\shell32.dll
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Config
 Opens:
                         C:\WINDOWS\system32\comctl32.dll
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Manifest
 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
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History\History.IE5
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Cookies
                         C:\Documents and Settings\Admin\Cookies\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\index.dat
                         C:\WINDOWS\system32\ws2_32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\ws2help.dll
 Opens:
                         C:\WINDOWS\system32\rasapi32.dll
                         C:\WINDOWS\system32\rasman.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\netapi32.dll
 Opens:
                         C:\WINDOWS\system32\tapi32.dll
                         C:\WINDOWS\system32\rtutils.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\TAPI32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\TAPI32.dll.124.Config
 Opens:
                         C:\AUTOEXEC.BAT
 Opens:
                         C:\Documents and Settings\All Users\Application
Data\Microsoft\Network\Connections\Pbk
 Opens:
                         C:\WINDOWS\system32\ras
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\Network\Connections\Pbk\
                         C:\WINDOWS\system32\sensapi.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\mswsock.dll
 Opens:
                         C:\WINDOWS\system32\rasadhlp.dll
 Opens:
                         C:\WINDOWS\system32\dnsapi.dll
 Opens:
                         C:\WINDOWS\system32\iphlpapi.dll
 Opens:
                         C:\WINDOWS\system32\drivers\etc\hosts
 Opens:
                         C:\WINDOWS\system32\rsaenh.dll
 Opens:
                         C:\WINDOWS\system32\msv1_0.dll
 Opens:
                         C:\WINDOWS\system32\crypt32.dll
 Opens:
                         C:\WINDOWS\system32\hnetcfg.dll
 Opens:
                         C:\WINDOWS\system32\wshtcpip.dll
 Opens:
                         C:\WINDOWS\system32\ieframe.dll
 Opens:
                         C:\Program Files\Internet Explorer\iexplore.exe
 Opens:
                         C:\WINDOWS\system32\ieframe.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\ieframe.dll.123.Config
                         C:\WINDOWS\system32\en-US\ieframe.dll.mui
 Opens:
 Opens:
                         C:\WINDOWS\system32
 Opens:
                         C:\WINDOWS
                         C:\WINDOWS\system32\setupapi.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\cmd.exe
 Opens:
                         C:\WINDOWS\AppPatch\sysmain.sdb
                         C:\WINDOWS\AppPatch\systest.sdb
 Opens:
 Opens:
                         C:\WINDOWS\system32\cmd.exe.Manifest
 Opens:
                         C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf
 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\svstem32\msvcrt.dll Opens: C:\WINDOWS\system32\user32.dll Opens: C:\WINDOWS\system32\gdi32.dll Opens: C:\WINDOWS\system32\shimeng.dll C:\WINDOWS\AppPatch\AcGenral.dll Opens: Opens: C:\WINDOWS\system32\advapi32.dll Opens: C:\WINDOWS\system32\rpcrt4.dll C:\WINDOWS\system32\secur32.dll Opens: 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:\WINDOWS\WINHELP.INI
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 C:\WINDOWS\system32\winlogon.exe Opens: Opens: C:\WINDOWS\system32\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\Registration\R00000000007.clb

Reads from: C:\WINDOWS\Temp\6f21fb21650da014d87426fa0bd8e7f2.exe

Reads from: C:\AUT0EXEC.BAT

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

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

Network Events

 DNS query:
 80170.z0dns.com

 Sends data to:
 8.8.8.8:53

 Receives data from:
 0.0.0.0:0

Windows Registry Events

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

folders

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

Creates key: HKLM\software\microsoft\tracing

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

folders

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

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

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

settings\connections

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

awareness

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

Creates key:

Creates key: HKLM\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
Creates key: HKCU\software\microsoft\windows\currentversion\shell extensions\cached

Creates key:

806d6172696f}\

 $\label{lem:condition} {\it Creates key:} \qquad \qquad {\it HKCU\software\microsoft\mbox{\sc multimedia\audio}}$

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

v4.00

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

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

settings[proxyserver]

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

settings[proxyoverride]

Deletes value:

HKCU\software\microsoft\windows\currentversion\internet

settings[autoconfigurl]

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

options\6f21fb21650da014d87426fa0bd8e7f2.exe

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

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

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

options\secur32.dll

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

options\rpcrt4.dll

Opens key:

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

options\advapi32.dll

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

Opens key:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} windows \ nt \current version \end{tabular} diagnostics$ Opens key:

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

options\user32.dll

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

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

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

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

options\gdi32.dll

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

options\winmm.dll

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

Opens key:

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

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

options\imm32.dll

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

options\msvcrt.dll

Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$

options\ole32.dll

HKLM\software\microsoft\ole Opens kev:

HKCR\interface Opens key:

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

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

options\oleaut32.dll

Opens key: HKLM\software\microsoft\oleaut

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

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

options\msvbvm60.dll

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

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

options\kernel32.dll

Opens key: HKCU\

Opens key: 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 key:

 $HKLM \setminus software \setminus microsoft \setminus ctf \setminus compatibility \setminus 6f21fb21650 da014 d87426 fa0bd8e7f2.exe$

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

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

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

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

options\version.dll

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

options\msctfime.ime

Opens key: HKCU\software\microsoft\ctf

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

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

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

Opens key: HKLM\software\microsoft\com3

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

options\comres.dll

 $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ Opens key:

options\clbcatq.dll

Opens key: HKLM\software\microsoft\com3\debug Opens key: HKCU\software\classes\ HKLM\software\classes Opens kev: Opens key: HKU\ Opens key: HKCR\clsid Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{85847f48 - d652 - 4fd3 - 9cd1 - 3ddafdba1a15\}$ HKCR\clsid\{85847f48-d652-4fd3-9cd1-3ddafdba1a15} Opens key: HKCU\software\classes\clsid\{a450fe5b-6ab7-4a3c-9cf3-3cee05d360c1} Opens key: Opens key: HKCR\clsid\{a450fe5b-6ab7-4a3c-9cf3-3cee05d360c1} HKCU\software\classes\clsid\{56d37229-f433-4eef-a6a7-b69dd0e003a3} Opens key: HKCR\clsid\{56d37229-f433-4eef-a6a7-b69dd0e003a3} Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{074c6e97 - 3f4e - 4659 - 9428 - 62a3d81a47c1\}$ Opens key: HKCR\clsid\{074c6e97-3f4e-4659-9428-62a3d81a47c1} HKCU\software\classes\clsid\{98e514e2-7646-40b7-9b56-9292aacf45cb} Opens key: Opens key: HKCR\clsid\{98e514e2-7646-40b7-9b56-9292aacf45cb} Opens key: HKCU\software\classes\clsid\{1ec267b1-9ab3-4fd2-840e-ec868c13387b} HKCR\clsid\{1ec267b1-9ab3-4fd2-840e-ec868c13387b} Opens kev: Opens key: HKCU\software\classes\clsid\{f3aaac74-c3f9-4f8e-a603-5e1ca200bf54} Opens key: HKCR\clsid\{f3aaac74-c3f9-4f8e-a603-5e1ca200bf54} Opens key: HKLM\system\currentcontrolset\services\disk\enum Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shlwapi.dll Opens kev: HKLM\software\microsoft\windows\currentversion\explorer\performance Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\normaliz.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\iertutil.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\urlmon.dll Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\comctl32.dll Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wininet.dll HKCU\software\classes\protocols\name-space handler\ Opens key: Opens key: HKCR\protocols\name-space handler Opens key: HKCU\software\classes\protocols\name-space handler Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} internet \end{tabular}$ settings Opens key: HKLM\software\microsoft\windows\currentversion\internet settings $\label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ Opens key: settings Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown HKLM\software\microsoft\internet explorer\main\featurecontrol\feature protocol lockdown HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\ HKLM\software\policies\microsoft\internet explorer\main\featurecontrol Opens key: Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol Opens kev: 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 kev: settings\zonemap\ranges\ Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\ HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_unc_savedfilecheck Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck HKLM\system\currentcontrolset\control\wmi\security Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\internet settings Opens key: HKLM\software\policies HKCU\software\policies Opens key: HKCU\software Opens kev: 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

HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache
 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 kev:
options\shell32.dll
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0\cache\history
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
 Opens key:
                         HKLM\software\microsoft\rpc\pagedbuffers
 Opens key:
                         HKLM\software\microsoft\rpc
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\6f21fb21650da014d87426fa0bd8e7f2.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
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\extensible cache\feedplat
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\extensible cache\iecompat
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\extensible cache\ietld
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\extensible cache\mshist012014033120140407
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\extensible cache\privacie:
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
                         HKLM\software\microsoft\internet
 Opens key:
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
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
 Opens key:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0\cache
 Opens key:
                         HKCU\software\microsoft\internet
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
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
                         HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens kev:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature permit cache for authenticated ftp kb910274
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens kev:
                         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 kev: 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 key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000 Opens kev: Opens key: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\wpad}} \\$ HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_http_username_password_disable Opens key: HKLM\software\microsoft\internet $explorer \verb|\main\featurecontrol\feature_http_username_password_disable|$ HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\netapi32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasman.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rtutils.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\tapi32.dll Opens key: HKLM\software\microsoft\windows\currentversion\telephony Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasapi32.dll Opens key: HKLM\software\microsoft\tracing\rasapi32

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution 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: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ profile list$ Opens key: HKLM\system\currentcontrolset\control\session manager\environment Opens key: ${\it HKLM \ } software \ \\ microsoft \ \\ windows \ \\ current version$

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003 Opens key: HKCU\environment Opens key: HKCU\volatile environment Opens key: $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ 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 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling HKLM\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_mime_handling Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mswsock.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasadhlp.dll HKCU\software\microsoft\windows\currentversion\internet Opens kev: 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\ HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\zonemap\protocoldefaults\ HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\zonemap\domains\ HKLM\software\microsoft\windows\currentversion\internet Opens key: settings\zonemap\domains\ HKLM\software\microsoft\windows\currentversion\internet Opens kev: settings\zonemap\domains\msn.com HKLM\software\microsoft\windows\currentversion\internet Opens key: settings\zonemap\domains\msn.com\related Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination Opens kev: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination HKCU\software\microsoft\internet explorer\ietld Opens kev: Opens key: HKLM\software\policies\microsoft\internet explorer\security Opens key: $\label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+internet settings \verb+\zones \verb++. \\$ Opens key: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\sl} zones \end{\tt 0}$ HKCU\software\microsoft\windows\currentversion\internet settings\zones\1 Opens kev: 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: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\ Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\0

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

settings\zones\0

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

settings\zones\1

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

settings\zones\1

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

settings\zones\2

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

settings\zones\2 Opens key:

 $\label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ settings\zones\3

Opens key:

HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\3

Opens kev:

HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\4

Opens key: $\label{lem:hkcu} \verb+KCU\software\policies\microsoft\windows\currentversion\currenters$

settings\zones\4

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

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

settings\lockdown_zones\

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

```
settings\lockdown_zones\
                                                HKCU\software\microsoft\windows\currentversion\internet
   Opens kev:
settings\lockdown_zones\
   Opens key:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                                                \label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} explicitly independent of the local property of the local propert
   Opens key:
settings\lockdown_zones\0
  Opens key:
                                               HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
   Opens key:
                                               HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
   Opens key:
                                                \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\1
                                               HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\1
   Opens key:
                                               HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
   Opens key:
                                                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
                                               HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\2
   Opens key:
                                               HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
   Opens key:
                                                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                                               HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\3
                                               HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\4
   Opens key:
                                                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
                                               HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\4
   Opens key:
                                               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
   Opens key:
                                                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
options\dnsapi.dll
   Opens key:
                                                HKLM\system\currentcontrolset\services\dnscache\parameters
   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
   Opens key:
                                                HKLM\system\currentcontrolset\services\tcpip\linkage
   Opens key:
                                                HKLM\system\currentcontrolset\services\tcpip\parameters\
                                                HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
   Opens key:
                                                HKLM\system\currentcontrolset\services\netbt\parameters
   Opens key:
   Opens key:
c7d49d7cecdc}
                                                HKLM\software\policies\microsoft\system\dnsclient
   Opens key:
   Opens key:
                                                HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
   Opens kev:
                                                HKLM\software\microsoft\rpc\securityservice
                                                Opens key:
   Opens key:
                                                HKLM\system\currentcontrolset\control\lsa\sspicache
   Opens key:
                                                HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll
                                                HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll
   Opens key:
   Opens key:
                                                HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll
   Opens key:
                                                HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
   Opens key:
                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msv1_0.dll
   Opens key:
                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rsaenh.dll
   Opens key:
                                                HKLM\software\policies\microsoft\cryptography
   Opens key:
                                                HKLM\software\microsoft\cryptography
                                                {\tt HKLM \ } software \ \verb|\ microsoft \ \verb|\ cryptography \ \verb|\ offload|
   Opens key:
   Opens key:
                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\hnetcfg.dll
                                                \label{lem:hklm} \verb+Kklm \+ services + winsock + parameters + winsock + wins
   Opens key:
   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:
HKLM \ software \ `microsoft \ 'windows \ 'current version' shell compatibility \ 'applications' \ '6f21fb21650 \ 'da014d87426 \ fa0bd8e7 \ f2.exe
   Opens key:
                                                HKCU\software\microsoft\windows\currentversion\explorer
   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 kev:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus desktop \setminus names pace
```

Opens key:

bc06-4ada335c892b}

Opens key:

ba4f-00a0c91eedba}

Opens key:

98a8-0800361b1103}

Opens key:

9f08-00aa002f954e}

Opens key:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ desktop \ names pace \ \{e17d4fc0-5564-11d1-e17d4fc0-5564$

83f2-00a0c90dc849}

Opens key:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current \lor version \setminus explorer \setminus desktop \setminus names pace$

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

Opens key:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus session info \setminus 0000000000008352 \setminus desktop \setminus names pace$

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}\shellfolder

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

08002b30309d}\shellfolder

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

Opens key:

HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{871c5380-42a0-1069-

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: 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

 $\label{lem:continuous} Opens \ key: \\ Opens \ key: \\ HKCQ \ Software \ classes \ clsid \ \{871c5380-42a0-1069-a2ea-8002b30309d\} \ treatas \\ Opens \ key: \\ HKCU \ Software \ classes \ clsid \ \{871c5380-42a0-1069-a2ea-8002b30309d\} \ treatas \\ Opens \ key: \\ Open$

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-

 $08002b30309d \} \verb|\inprochandler32|$

 $Opens~key: \\ HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\ \ inprochandler 32 \\$

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

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

Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
Opens key: HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc-

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\{000214e6-0000-0000-0000-00000000046}\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: HKCR\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder

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

```
00a0c91eedba}\shellfolder
                                        HKCR\clsid\{1f4de370-d627-11d1-ba4f-00a0c91eedba}\shellfolder
  Opens key:
  Opens key:
                                        HKCU\software\classes\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder
  Opens kev:
                                        HKCR\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder
  Opens key:
                                        HKCU\software\classes\clsid\{645ff040-5081-101b-9f08-
00aa002f954e}\shellfolder
                                        HKCR\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder
  Opens key:
  Opens key:
                                        HKCU\software\classes\clsid\{e17d4fc0-5564-11d1-83f2-
00a0c90dc849}\shellfolder
                                        HKCR\clsid\{e17d4fc0-5564-11d1-83f2-00a0c90dc849}\shellfolder
  Opens kev:
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\shellexecutehooks
  Opens key:
                                        HKCU\software\classes\clsid\{aeb6717e-7e19-11d0-97ee-
00c04fd91972}\inprocserver32
  Opens key:
                                        HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32
                                        HKLM\software\microsoft\windows\currentversion\app paths\cmd.exe
  Opens kev:
  Opens key:
                                        HKLM\software\microsoft\windows\currentversion\policies\associations
  Opens key:
                                        HKCU\software\microsoft\windows\currentversion\policies\associations
                                        HKCU\software\classes\.exe
  Opens key:
  Opens key:
                                        HKCR\.exe
  Opens key:
                                        HKCU\software\classes\.ade
                                        HKCR\.ade
  Opens kev:
  Opens key:
                                        HKCU\software\classes\.adp
  Opens key:
                                        HKCR\.adp
                                        HKCU\software\classes\.app
  Opens key:
  Opens key:
                                        HKCR\.app
  Opens key:
                                        HKCU\software\classes\.asp
  Opens key:
                                        HKCR\.asp
  Opens key:
                                        HKCU\software\classes\.bas
  Opens key:
                                        HKCR\.bas
                                        HKCU\software\classes\.bat
  Opens key:
  Opens key:
                                        HKCR\.bat
  Opens key:
                                        HKCU\software\classes\.cer
  Opens key:
                                        HKCR\.cer
  Opens key:
                                        HKCU\software\classes\.chm
  Opens key:
                                        HKCR\.chm
                                        HKCU\software\classes\.cmd
  Opens key:
  Opens key:
                                        HKCR\.cmd
  Opens key:
                                        HKCU\software\classes\.com
  Opens key:
                                        HKCR\.com
  Opens key:
                                        HKCU\software\classes\.cpl
  Opens kev:
                                        HKCR\.cpl
  Opens key:
                                        HKCU\software\classes\.crt
  Opens key:
                                        HKCR\.crt
  Opens key:
                                        HKCU\software\classes\.csh
  Opens key:
                                        HKCR\.csh
  Opens key:
                                        HKCU \setminus software \setminus classes \setminus clsid \setminus \{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4\}
                                        HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
  Opens kev:
  Opens key:
                                        HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\treatas
                                        HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas
  Opens kev:
  Opens key:
                                        HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32
                                        HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32
  Opens kev:
  Opens key:
                                        HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserverx86
                                        HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserverx86
  Opens key:
                                        HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
  Opens key:
00c04fb6bfc4}\localserver32
  Opens key:
                                        HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver32
  Opens key:
                                        HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler32
                                        HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32
  Opens kev:
  Opens key:
                                        HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandlerx86
  Opens key:
                                        HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandlerx86
                                        HKCU \setminus software \setminus classes \setminus clsid \setminus \{7b8a2d94 - 0ac9 - 11d1 - 896c - 11d1 - 806c - 1
  Opens key:
00c04fb6bfc4}\localserver
                                        HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver
  Opens kev:
  Opens key:
                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610
                                        HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610
  Opens key:
                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
  Opens key:
                                        HKLM\software\microsoft\internet
```

Opens key:

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

Opens key: HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32

explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000

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

options\setupapi.dll

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

Opens key: HKLM\svstem\wpa\pnp

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

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

Opens key:

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

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{f90255c2-6bc4-f9025fc2-$

11e3-9fc7-806d6172696f}\

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

HKCR\drive\shellex\folderextensions Opens key:

Opens key: HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-

4442-804e-409d6c4515e9}

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

409d6c4515e9}

Opens key: HKCU\software\classes\directory

HKCR\directory Opens key:

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

Opens key: HKCR\directory\curver HKCR\directory\ Opens kev:

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

Opens key: HKCU\software\classes\directory\shellex\iconhandler

Opens key: HKCR\directory\shellex\iconhandler Opens key: HKCU\software\classes\directory\clsid

Opens key: HKCR\directory\clsid

HKCU\software\classes\folder Opens key:

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 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.exe

HKCU\software\classes\exefile Opens key:

Opens key: HKCR\exefile

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

HKCR\exefile\curver Opens key:

Opens key: HKCR\exefile\

Opens key: HKCU\software\classes\exefile\shellex\iconhandler

HKCR\exefile\shellex\iconhandler Opens key:

Opens key: HKCU\software\classes\systemfileassociations\.exe

Opens key: HKCR\systemfileassociations\.exe

 ${\tt HKCU \setminus software \setminus classes \setminus system file associations \setminus application}$ Opens key:

Opens key: HKCR\systemfileassociations\application HKCU\software\classes\exefile\clsid Opens key:

HKCR\exefile\clsid Opens key: Opens key: HKCU\software\classes*

HKCR* Opens kev:

HKCU\software\classes*\clsid Opens key:

Opens key: HKCR*\clsid

Opens key: HKCU\software\classes\exefile\shell

Opens key: HKCR\exefile\shell

Opens key: HKCU\software\classes\exefile\shell\open

Opens kev: HKCR\exefile\shell\open

Opens key: HKCU\software\classes\exefile\shell\open\command

Opens key: HKCR\exefile\shell\open\command

Opens key:

HKCU\software\microsoft\windows\currentversion\policies\explorer\restrictrun

Opens key: HKCU\software\classes\exefile\shell\open\ddeexec

Opens key: HKCR\exefile\shell\open\ddeexec

HKCU\software\classes\applications\cmd.exe Opens key:

Opens key: HKCR\applications\cmd.exe

Opens key: HKCU\software\microsoft\windows\shellnoroam

HKCU\software\microsoft\windows\shellnoroam\muicache Opens key: Opens key: HKCU\software\microsoft\windows\shellnoroam\muicache\

Opens key:

Opens key: HKLM\system\wpa\tabletpc Opens key: HKLM\system\wpa\mediacenter

 ${\tt HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus app compatflags \setminus layers}$ Opens key:

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 kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths

Opens key:

be2efd2c1a33}

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes

Opens key:

edd5fbde1328}

Opens key:

Opens key:

 $\label{thm:local-bound} HKLM\software\policies\microsoft\windows\safer\codeidentifiers\olines\colored{HKLM-software} Ald1fe15-dd9d-4762-b16d-7c29ddecae3f}$

Opens key:

Opens kev:

Opens key:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:local_hammon} soft \end{tabular} windows \end{tabular} soft \end{tabular} windows \end{tabular} and \end{tabular} is the local property of the local p$

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
 Opens kev:

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:

 $\label{thm:hklm} HKLM \software \policies \microsoft \windows \safer \code identifiers \code \ \code$

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
 Opens kev:

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 kev:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones

Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
Opens kev:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
Opens kev:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes

Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones Opens key:

 $\label{lem:hkcu} HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths \\ Opens\ key:$

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
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\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
Opens key:

 $\label{lem:hkcu} HKCU\software\policies\microsoft\windows\safer\codeidentifiers\normalfootnotes Opens\ key:$

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
 Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

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

options\acgenral.dll
Opens key

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

options\shimeng.dll

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

options\msacm32.dll

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

options\uxtheme.dll

Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache

Opens kev:

 $\label{thm:limit} \begin{tabular}{ll} HKLM \end{tabular} in a addition of the limit of the lim$

Opens key:

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

Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711

Opens key:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610

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

Opens key:

 $HKLM \verb|\software\m| icrosoft\audio compression manager\driver cache \verb|\m| sacm. msaudio 1 \\$

Opens key:

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

Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.13acm

Opens key: HKLM\system\currentcontrolset\control\mediaresources\acm
Opens key: HKCU\software\microsoft\windows\currentversion\thememanager

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\currentcontrol\set\control\nls\locale

Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts

Opens key: HKLM\system\currentcontrolset\control\nls\language groups

 $\label{lem:constraint} Opens \ key: \\ HKLM \ software \ microsoft \ windows \\ nt \ current version \ approximation \ custom \ task \ list. exe$

Opens key: HKLM\software\microsoft\windows nt\currentversion\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 key: HKLM\software\microsoft\ctf\compatibility\tasklist.exe

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

options\tasklist.exe\rpcthreadpoolthrottle

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

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

options\xpsp2res.dll

Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}

Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\treatas

00aa004b2e24}\inprocserver32

 $Opens~key: \\ HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\ \ \ inprocserver32$

Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\inprocserverx86

Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-

 $00aa004b2e24 \} \\ local server 32$

Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\localserver32

Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\inprochandler32

Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler32

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

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

options\wbemcomn.dll

Opens key: ${\tt HKLM \backslash software \backslash microsoft \backslash windows\ nt \backslash current version \backslash image\ file\ execution}$

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}

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

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

00c04fb68820}\treatas

00c04fb68820}\inprocserver32

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

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

00c04fb68820}\inprocserverx86

Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserverx86

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

00c04fb68820}\localserver32

Opens key: $\label{eq:hkcr} \mbox{HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820\}\localserver32}} \mbox{ } \mbox{ } \mbox{localserver32} \mbox{ } \mbox{ } \mbox{localserver32} \mbox{ } \mbo$

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

```
00c04fb68820}\inprochandler32
```

Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandler32

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

00c04fb68820}\inprochandlerx86

Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandlerx86

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

00c04fb68820}\localserver

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

Opens key: HKCU\software\classes\interface\{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

 $\label{lem:continuous} Opens \ key: \ HKCR \ HKCR \ HKCR \ HKCU \ Software \ Classes \ 140-a075-00c04fb68820 \ Proxystubclsid32 \ HKCU \ Software \ Classes \ 17c87801-7381-11cf-884d-00aa004b2e24 \ HKCU \ Software \ New \$

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

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

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

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: $\label{eq:hcclsid} $$ HKCR\clsid_{d68af00a-29cb-43fa-8504-ce99a996d9ea}\times Opens key: $$ HKCU\software\classes\clsid_{d68af00a-29cb-43fa-8504-} $$$

ce99a996d9ea}\inprocserver32

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

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

ce99a996d9ea}\inprocserverx86

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

Opens key: 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-

ce99a996d9ea}\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: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\fastprox.dll

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

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

00000000001}\proxystubclsid32

Opens key: $\label{eq:hkcr} \begin{tabular}{ll} HKCR\interface\{0.027947e1-d731-11ce-a357-00000000001\}\proxystubclsid32\\ Opens key: \\ HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd} \end{tabular}$

 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}\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

Opens key: $\label{eq:hccv} \begin{tabular}{ll} HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}\proxystubclsid32\\ Opens key: \\ HKCU\software\classes\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\end{tabular}$

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\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]

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[safedllsearchmode]

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

nt\currentversion\compatibility32[6f21fb21650da014d87426fa0bd8e7f2]

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

compatibility[6f21fb21650da014d87426fa0bd8e7f2]

Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2] HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3] Queries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5] Oueries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6] Oueries value: $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [midi7]$ Queries value: $HKLM \backslash software \backslash microsoft \backslash windows \ nt \backslash current version \backslash drivers 32 [midi8]$ Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux] $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [aux 1]$ Oueries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9] Queries value:

HKLM\system\currentcontrol\set\control\mediaproperties\privateproperties\joystick\winmm[wheel]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]

```
Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32\mixer51
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
  Oueries value:
                           HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
  Queries value:
                           HKLM\software\microsoft\ole[rwlockresourcetimeout]
  Queries value:
                           HKCR\interface[interfacehelperdisableall]
  Oueries value:
                           HKCR\interface[interfacehelperdisableallforole32]
  Queries value:
                           HKCR\interface[interfacehelperdisabletypelib]
  Oueries value:
                           HKCR\interface\{00020400-0000-0000-c000-
00000000046}[interfacehelperdisableall]
  Queries value:
                           HKCR\interface\{00020400-0000-0000-c000-
00000000046}[interfacehelperdisableallforole32]
                           HKCU\control panel\desktop[multiuilanguageid]
  Queries value:
  Queries value:
                           HKLM\software\microsoft\ctf\systemshared[cuas]
  Queries value:
                           HKCU\keyboard layout\toggle[language hotkey]
                           HKCU\keyboard layout\toggle[hotkey]
  Oueries value:
  Queries value:
                           HKCU\keyboard layout\toggle[layout hotkey]
  Queries value:
                           HKLM\software\microsoft\ctf[enableanchorcontext]
                           HKLM\system\currentcontrolset\control\session
  Queries value:
manager[safeprocesssearchmode]
                           HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
  Queries value:
                           HKCU\software\microsoft\ctf[disable thread input manager]
  Oueries value:
  Queries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[932]
  Queries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[949]
  Queries value:
                           HKLM\system\currentcontrolset\control\nls\codepage[950]
                           HKLM\system\currentcontrolset\control\nls\codepage[936]
  Queries value:
  Queries value:
                           HKLM\software\microsoft\com3[com+enabled]
                           HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
  Oueries value:
                           {\tt HKLM \setminus software \setminus microsoft \setminus ole[minimumfreemempercentage to create object]}
  Queries value:
                           HKLM\software\microsoft\com3[regdbversion]
  Oueries value:
  Oueries value:
                           HKLM\system\currentcontrolset\services\disk\enum[0]
                           HKCU\control panel\desktop[smoothscroll]
  Queries value:
  Queries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus advanced [enable balloon tips]
                           \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
  Queries value:
settings[disableimprovedzonecheck]
  Queries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[6f21fb21650da014d87426fa0bd8e7f2.exe]
                           HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_protocol_lockdown[*]
  Queries value:
                           ab78-1084642581fb]
                           Queries value:
0000-000000000000000
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[fromcachetimeout]
  Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[secureprotocols]
  Queries value:
                           HKLM\software\policies\microsoft\internet
explorer\main[security_hklm_only]
  Oueries 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[certificaterevocation]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablekeepalive]
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Oueries value:
settings[idnenabled]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[cachemode]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[proxyhttp1.1]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[enablenegotiate]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablebasicoverclearchannel]
                           HKCU\software\microsoft\internet
  Oueries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
  Oueries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol[feature clientauthcertfilter]
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[syncmode5]
```

```
Oueries value:
                                      HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
  Queries value:
                                      \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma of the 
settings\5.0\cache[signature]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\content[peruseritem]
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
  Queries value:
                                      HKLM\system\setup[systemsetupinprogress]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
  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\content[cacheprefix]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\content[cachelimit]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
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]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\cookies[cachelimit]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\history[peruseritem]
                                      HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\history[peruseritem]
                                      HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Queries value:
folders[historv]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\history[cacheprefix]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
                                      HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
  Oueries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\domstore[cacherepair]
  Queries value:
                                      \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings\5.0\cache\extensible cache\domstore[cachepath]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
  Oueries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
  Queries value:
                                      \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings\5.0\cache\extensible cache\domstore[cacheoptions]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\feedplat[cacherepair]
  Oueries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\feedplat[cachelimit]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\iecompat[cachepath]
                                     \label{thm:linear} \verb+HKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachelimit]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\ietld[cacheprefix]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
  Queries value:
                                      \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\extensible cache\ietld[cacheoptions]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
```

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

```
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cacherepair]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cachepath]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cachelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablereadrange]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketsendbufferlength]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketreceivebufferlength]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[keepalivetimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsper1_0server]
 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[maxconnectionsperproxy]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connecttimeout]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
 Queries value:
                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[connectretries]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connectretries]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendtimeout]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[receivetimeout]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[receivetimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablentlmpreauth]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[scavengecachelowerbound]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelimit]
 Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[httpdefaultexpirytimesecs]
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Oueries value:
settings[ftpdefaultexpirytimesecs]
```

```
Queries value:
                             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[6f21fb21650da014d87426fa0bd8e7f2.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]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
                             HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[disablent4rascheck]
                             HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dialupuselansettings]
                             HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dialupuselansettings]
                             HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[sendextracrlf]
                             HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypassftptimecheck]
                             HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[releasesocketduringauth]
                             HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[releasesocketduring401auth]
                             HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[releasesocketduring401auth]
                             HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[wpadsearchalldomains]
  Oueries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
                             HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablelegacypreauthasserver]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
  Queries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasssslnocachecheck]
                             HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasssslnocachecheck]
  Queries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[nocheckautodialoverride]
  Oueries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Oueries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Oueries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[headerexclusionlistforcache]
  Oueries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
                             \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
  Queries value:
settings[dnscacheentries]
                             HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dnscachetimeout]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonzonecrossing]
  Queries value:
                             \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[warnonbadcertsending]
  Queries value:
                             \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[warnonbadcertrecving]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonpostredirect]
  Queries value:
                             \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[alwaysdrainonredirect]
                             \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
  Queries value:
settings[warnonhttpstohttpredirect]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Queries value:
```

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
 Queries value:
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
- Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000011[packedcatalogitem]
- Queries value:
- $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \names pace_catalog 5 [serial_access_num] \\ Queries \value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
- Queries value: HKCU\software\microsoft\windows\currentversion\internet
- settings[globaluseroffline]

```
Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
                         HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus internet
 Queries value:
settings[urlencoding]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[truncatefilename]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[badproxyexpirestime]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32maxnumrequestretries]
 Oueries value:
Oueries value:
                         HKLM\software\microsoft\tracing[enableconsoletracing]
                         HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
 Oueries value:
 Queries value:
                         HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
 Queries value:
                         HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
                         HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
 Oueries value:
 Queries value:
                         HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
 Queries value:
                         HKLM\software\microsoft\tracing\rasapi32[filedirectory]
 Oueries value:
                         HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common appdata]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\winlogon[chkaccdebuglevel]
                         HKLM\system\currentcontrolset\control\productoptions[producttype]
 Oueries value:
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[personal]
                         HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Oueries value:
folders[local settings]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\winlogon[rsopdebuglevel]
                         HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
 Queries value:
 Queries value:
                         HKLM\software\microsoft\windows
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:
 Oueries value:
                         HKLM\software\microsoft\windows\currentversion[commonfilesdir]
                         Queries value:
1757981266-507921405-1957994488-1003[profileimagepath]
                         HKCU\software\microsoft\windows
 Queries value:
nt\currentversion\winlogon[parseautoexec]
                         HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Queries value:
folders[appdata]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxv]
 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
 Queries value:
settings\connections[defaultconnectionsettings]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[6f21fb21650da014d87426fa0bd8e7f2.exe]
                         HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature mime handling[*]
                         HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
 Oueries value:
 Queries value:
                         HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
 Oueries value:
                         HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
 Queries value:
                         HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[flags]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[flags]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\4[flags]
 Queries value:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[6f21fb21650da014d87426fa0bd8e7f2.exe]
```

HKCU\software\microsoft\internet

```
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
                          HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[6f21fb21650da014d87426fa0bd8e7f2.exe]
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
 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:
                          \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
settings[enablepunycode]
                          \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
 Queries value:
settings\zonemap[autodetect]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\3[1a10]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [prioritize record data]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [prioritize record data]
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [allow unqualified query]
 Queries value:
HKLM \ system \ (current control set \ services \ dns cache \ parameters [append to multilabel name]
HKLM\svstem\currentcontrolset\services\dnscache\parameters[screenbadtlds]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [filter clusterip]
HKLM\svstem\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
 Queries value:
                          HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
 Queries value:
                          HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
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]
 Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
```

Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[updatetop]eveldomainzones]

Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]

Queries value:

Oueries value:

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

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [server priority time limit]$

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [max cached sockets]$

Queries value:

 $\label{local-parameters} $$HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]$$$

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [multicast send level]$

Queries value:

 ${\tt HKLM \ } system \verb| current control set \verb| services \verb| tcpip \verb| parameters [dns query time outs]|$

Queries value:

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

Queries value:

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

Queries value:

c7d49d7cecdc}[enabledhcp]

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [lease obtained time]$

Oueries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [lease terminates time]$

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \troip \parameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [dhcpserver]$

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

 $\label{local-hkl} HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [queryadaptername]$

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \troip \parameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [disable adapter domain name]$

Oueries value:

 $\label{thm:local-set-services} HKLM \system \current controls et \services \tcpip \parameters \time faces \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} [registration enabled]$

Queries value:

 $HKLM \ system \ `controlset \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [register adapter name]$

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \true \parameters \end{16325b0b-4636-4303-abe3-c7d49d7cecdc} \parameters \parame$

Queries value:

 $\label{local-equation} HKLM \system \current control set \services \true \parameters \end{2.0} In the faces \end{2.0} abe 3-abe 3-$

Oueries value:

 $\label{lem:hklmsystem} HKLM \system \critector \crite$

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpdomain]

Queries value:

 $\label{local-ham} HKLM \system \current control set \services \true pharameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} [ipautoconfiguration enabled]$

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[addresstype]

Queries value:

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \tcpip \parameters \interfaces \{16325b0b-4636-4303-abe3-c7d49d7cecdc\}[dhcpnameserver]$

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

Queries value:

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

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

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

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

```
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
    Oueries value:
                                                              HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
    Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]
    Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]
    Oueries value:
                                                              HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]
    Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[version]
                                                              HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]
    Queries value:
    Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]
    Queries value:
                                                              HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]
                                                              HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]
    Oueries value:
    Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities]
                                                              HKLM \setminus system \setminus current control \\ \  \setminus sspicache \setminus digest. \\ dll[rpcid]
    Oueries value:
    Queries value:
                                                              HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version]
    Queries value:
                                                              HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]
    Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize]
                                                              HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name]
    Queries value:
                                                              Oueries value:
    Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities]
                                                              \label{lem:hklm} \verb+Kklm \+ system \+ control \+ lsa \+ spicache \+ msnsspc.dll[rpcid]
    Queries 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\software\microsoft\cryptography[machineguid]
                                                              HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
    Queries value:
    Queries value:
                                                              HKLM\system\currentcontrolset\services\winsock\parameters[transports]
    Queries value:
                                                              HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
    Oueries value:
                                                              HKLM\system\currentcontrolset\services\netbt\linkage[export]
    Queries value:
                                                              HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps]
                                                              HKLM\software\microsoft\windows\currentversion\explorer[maximizeapps]
    Oueries value:
    Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
    Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
bc06-4ada335c892b}[suppressionpolicy]
    Oueries value:
ba4f-00a0c91eedba}[suppressionpolicy]
HKLM \ software \ microsoft \ windows \ current version \ explorer \ desktop \ names pace \ \{450d8fba-ad25-11d0-day \ names 
98a8-0800361b1103}[suppressionpolicy]
HKLM \setminus software \setminus irrosoft \setminus ir
9f08-00aa002f954e}[suppressionpolicy]
HKLM \ software \ microsoft \ windows \ current version \ explorer \ desktop \ names pace \ \{e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564
83f2-00a0c90dc849}[suppressionpolicy]
    Queries value:
                                                              HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsparsedisplayname]
    Queries value:
                                                              HKCR\clsid\{208d2c60-3aea-1069-a2d7-
08002b30309d}\shellfolder[wantsparsedisplayname]
    Oueries value:
                                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsparsedisplayname]
    Queries value:
                                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[]
    Oueries value:
                                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[loadwithoutcom]
    Oueries value:
                                                              HKLM\software\microsoft\windows\currentversion\shell
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
    Oueries value:
                                                              HKCU\software\microsoft\windows\currentversion\shell
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
    Oueries value:
```

```
Oueries value:
                                                               HKLM\software\microsoft\windows\currentversion\shell
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}
0x4011
    Queries value:
                                                               HKCU\software\microsoft\windows\currentversion\shell
extensions \\ \\ cached [\{871c5380-42a0-1069-a2ea-08002b30309d\} \\ \\ \{000214e6-0000-0000-c000-0000000000046\} \\ \\ \\ \\ extensions \\ \\ \\ extensions \\ \\ extensio
0x4011
    Oueries value:
                                                               HKLM\system\currentcontrolset\control\session
manager\appcompatibility[disableappcompat]
                                                               HKCR\clsid\{871c5380-42a0-1069-a2ea-
    Oueries value:
08002b30309d}\inprocserver32[inprocserver32]
                                                               HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[appid]
    Oueries value:
    Queries value:
                                                               HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[threadingmodel]
    Oueries value:
                                                              HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe[]
    Oueries value:
                                                               HKLM\software\microsoft\internet explorer\setup[iexplorelastmodifiedlow]
    Queries value:
                                                               HKLM\software\microsoft\internet
explorer\setup[iexplorelastmodifiedhigh]
                                                               HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib[]
    Queries value:
    Oueries value:
                                                               HKLM\software\microsoft\internet explorer\setup[installstarted]
    Oueries value:
                                                               HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32[]
    Queries value:
                                                               HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32[]
    Queries value:
                                                               HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32[]
                                                               HKCR \verb|\interface| \{93f2f68c-1d1b-11d3-a30e-00c04f79abd1\} \verb|\proxystubclsid32[]| \\
    Oueries value:
                                                               HKCR\clsid\{11016101-e366-4d22-bc06-
    Queries value:
4ada335c892b}\shellfolder[wantsparsedisplayname]
                                                              HKCR\clsid\{1f4de370-d627-11d1-ba4f-
    Queries value:
00a0c91eedba}\shellfolder[wantsparsedisplayname]
    Queries value:
                                                               HKCR\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder[wantsparsedisplayname]
                                                              HKCR\clsid\{645ff040-5081-101b-9f08-
    Queries value:
00aa002f954e}\shellfolder[wantsparsedisplayname]
                                                              HKCR\clsid\{e17d4fc0-5564-11d1-83f2-
    Queries value:
00a0c90dc849}\shellfolder[wantsparsedisplayname]
    Queries value:
                                                              HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32[]
    Oueries value:
                                                              HKCR\clsid\{aeb6717e-7e19-11d0-97ee-
00c04fd91972}\inprocserver32[loadwithoutcom]
                                                              HKCR\.exe[]
    Oueries value:
                                                              HKCR\.asp[]
    Oueries value:
                                                               HKCR\.bat[]
    Queries value:
    Queries value:
                                                               HKCR\.cer[]
                                                              HKCR\.chm[]
    Oueries value:
                                                               HKCR\.cmd[]
    Queries value:
                                                               HKCR\.com[]
    Oueries value:
    Queries value:
                                                               HKCR\.cpl[]
                                                               HKCR\.crt[]
    Oueries value:
                                                              HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
    Queries value:
00c04fb6bfc4}\inprocserver32[inprocserver32]
    Queries value:
                                                               HKCR \c1sid \f3b8a2d94-0ac9-11d1-896c-00c04fb6bfc4 \c1sid \f3b8a2d94-0ac9-11d1-896c-00c04fb6bfc4 \c1sid \
                                                               HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[appid]
    Oueries value:
    Queries value:
                                                              HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[threadingmodel]
                                                              HKCU\software\microsoft\windows\currentversion\internet
    Oueries value:
settings[specialfolderscachesize]
    Queries value:
                                                              HKLM\software\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
    Queries value:
                                                              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1806]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
    Oueries value:
                                                               HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[]
    Queries value:
                                                               HKLM\system\wpa\pnp[seed]
    Oueries value:
                                                               HKLM\svstem\setup[osloaderpath]
    Queries value:
                                                               HKLM\system\setup[systempartition]
                                                               HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
    Queries value:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus setup [service packs our cepath]
    Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]
    Queries value:
                                                               HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
                                                               HKLM\software\microsoft\windows\currentversion[devicepath]
    Oueries value:
    Oueries value:
                                                               HKLM\software\microsoft\windows\currentversion\setup[loglevell
    Queries value:
                                                               HKLM\software\microsoft\windows\currentversion\setup[logpath]
    Queries value:
HKCU \ software \ microsoft \ windows \ current version \ \ explorer \ mountpoints 2 \ cpc \ \ \ \{f90255c2-6bc4-f8025f2, f8025f2, f8025f
11e3-9fc7-806d6172696f}[data]
11e3-9fc7-806d6172696f}[generation]
```

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

409d6c4515e9}[drivemask] Queries value:

```
HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
                                                HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
   Oueries value:
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[forceactivedesktopon]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell]
   Oueries 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]
                                                HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
   Oueries value:
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
   Queries value:
HKCU \ software \ microsoft \ windows \ current version \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ advanced \ advanced \ advanced \ (explorer \ advanced \ advanced \ advanced \ advanced \ (explorer \ advanced \ advanced \ advanced \ advanced \ (explorer \ advanced \ advanced \ advanced \ advanced \ (explorer \ advanced \ advanced \ advanced \ advanced \ (explorer \ advanced \ advanced \ advanced \ advanced \ (explorer \ advanced \ advanced \ advanced \ advanced \ (explorer \ advanced \ advanced \ advanced \ advanced \ advanced \ advanced \ (explorer \ advanced \ advanced \ advanced \ advanced \ advanced \ advanced \ (explorer \ advanced \ (explorer \ advanced \ (explorer \ advanced \ advance
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
   Queries value:
                                                HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
                                                HKCR\directory[docobject]
   Queries value:
   Queries value:
                                                HKCR\directory[browseinplace]
   Oueries value:
                                                HKCR\directory[isshortcut]
   Queries value:
                                                 HKCR\directory[alwaysshowext]
   Oueries value:
                                                HKCR\directory[nevershowext]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]
                                                HKCR\exefile[docobject]
   Queries value:
   Queries value:
                                                HKCR\exefile[browseinplace]
   Queries value:
                                                 HKCR\exefile[isshortcut]
   Oueries value:
                                                HKCR\exefile[alwaysshowext]
   Queries value:
                                                HKCR\exefile[nevershowext]
   Oueries value:
                                                HKCR\exefile\shell[]
   Oueries value:
                                                HKCR\exefile\shell\open\command[]
   Queries value:
                                                HKCR\exefile\shell\open\command[command]
   Queries value:
                                                1757981266-507921405-1957994488-1003[flags]
   Queries value:
                                                HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[state]
   Oueries value:
                                                HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[userpreference]
                                                HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
   Queries value:
1757981266-507921405-1957994488-1003[centralprofile]
   Queries value:
                                                HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus profile list \setminus s-1-5-21-1000 + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2) + (-5-2)
1757981266-507921405-1957994488-1003[profileloadtimelow]
                                                HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
   Oueries value:
1757981266-507921405-1957994488-1003[profileloadtimehigh]
                                                HKCU\software\microsoft\windows\shellnoroam\muicache[langid]
   Queries value:
HKCU \ software \ microsoft \ windows \ shell no roam \ muicache \ [c:\windows \ system 32 \ cmd. exe]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[inheritconsolehandles]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[disallowrun]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[norunasinstallprompt]
   Queries value:
                                                HKLM\system\wpa\mediacenter[installed]
   Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
                                                HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
   Oueries value:
   Queries value:
be2efd2c1a33}[itemdata]
```

Oueries value:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus paths \setminus \{dda3f824 - d8cb - 441b - 834d - d8cb - 441b - 441$ be2efd2c1a33}[saferflags]

Queries value:

edd5fbde1328}[itemdata]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89edd5fbde1328}[hashalg]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89edd5fbde1328}[itemsize]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89edd5fbde1328}[saferflags]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57bb813f72dbb91}[itemdata]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57bb813f72dbb91}[hashalg]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57bb813f72dbb91}[itemsize]

Queries value:

b813f72dbb91}[saferflags]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[itemdata]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[hashalg]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[itemsize]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[saferflags]

Queries value:

085bcc18a68d}[itemdata]

Oueries value:

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

Queries value:

085bcc18a68d}[itemsize]

Oueries value:

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

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe$ b91490411bfc}[itemdata]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2eb91490411bfc}[hashalg]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2eb91490411bfc}[itemsize]

Queries value:

 $HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae$ b91490411bfc}[saferflags]

Oueries value:

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

Oueries value:

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

Queries value: $\label{lem:hkcu} \verb+KKCU\+ software\+ icrosoft\+ windows\+ current version\+ explorer\+ shell$

folders[cache] Oueries value:

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

 $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus compatibility 32 [cmd]$ Oueries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[cmd] Oueries value:

Queries value: HKCU\software\microsoft\multimedia\audio[systemformats]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\drivers32[msacm.imaadpcm]

Queries value:

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

Oueries value:

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

Queries value:

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

```
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cfiltertags]
                       HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\drivers32[msacm.msadpcm]
 Queries value:
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cformattags]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[aformattagcache]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cfiltertags]
                       HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\drivers32[msacm.msg711]
 Oueries value:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msg711[fdwsupport]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cformattags]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cfiltertags]
                       HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\drivers32[msacm.msgsm610]
 Queries value:
Queries value:
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msgsm610 [cformattags]
 Queries value:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. msgsm610 [a formattag cache]
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cfiltertags]
 Queries value:
                       HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.trspch]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport]
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cformattags]
 Oueries value:
Queries value:
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. trspch[cfilter tags]
                       HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msg7231
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[fdwsupport]
 Queries value:
HKLM \verb|\software| microsoft| audiocompression manager| driver cache \verb|\msacm.msg723| [cformattags]|
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[aformattagcachel
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cfiltertags]
                       HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\drivers32[msacm.msaudio1]
 Queries value:
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cformattags]
 Oueries value:
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msaudio1[cfilter tags]
 Oueries value:
                       HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.sl anet]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[fdwsupport]
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cformattags]
 Queries value:
Oueries value:
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. sl\_anet [cfilter tags]
 Oueries value:
                       HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2]
 Oueries value:
HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus msacm.iac2[fdwsupport]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cformattags]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[aformattagcache]
 Oueries 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 \ audio compression manager \ driver cache \ msacm. 13 acm [fdw support]
```

```
Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cformattags]
  Oueries value:
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
  Queries value:
v4.00[priority1]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
  Queries value:
                                   HKCU\control panel\desktop[lamebuttontext]
  Oueries value:
                                   HKLM\software\microsoft\command processor[disableunccheck]
  Oueries value:
                                   HKLM\software\microsoft\command processor[enableextensions]
  Oueries value:
                                   HKLM\software\microsoft\command processor[delayedexpansion]
                                   HKLM\software\microsoft\command processor[defaultcolor]
  Oueries value:
  Oueries value:
                                   HKLM\software\microsoft\command processor[completionchar]
  Queries value:
                                   HKLM\software\microsoft\command processor[pathcompletionchar]
  Oueries value:
                                   HKLM\software\microsoft\command processor[autorun]
  Oueries value:
                                   HKCU\software\microsoft\command processor[disableunccheck]
  Queries value:
                                   HKCU\software\microsoft\command processor[enableextensions]
  Queries value:
                                   HKCU\software\microsoft\command processor[delayedexpansion]
                                   HKCU\software\microsoft\command processor[defaultcolor]
  Oueries value:
  Queries value:
                                   HKCU\software\microsoft\command processor[completionchar]
  Queries value:
                                   HKCU\software\microsoft\command processor[pathcompletionchar]
  Oueries value:
                                   HKCU\software\microsoft\command processor[autorun]
  Queries value:
                                   Queries value:
                                   HKLM\system\currentcontrolset\control\nls\language groups[1]
                                   HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\compatibility32[tasklist]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[tasklist]
  Queries value:
                                   HKLM\software\microsoft\wbem\cimom[logging]
  Queries value:
                                   HKLM\software\microsoft\wbem\cimom[logging directory]
  Oueries 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]
                                   HKCR\clsid\{4590f811-1d3a-11d0-891f-
  Oueries value:
00aa004b2e24}\inprocserver32[inprocserver32]
  Queries value:
                                   HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32[]
  Oueries value:
                                   \label{local-equation-bound} \mbox{HKCR\clsid} \mbox{\{4590f811-1d3a-11d0-891f-00aa004b2e24\}[appid]}
  Queries value:
                                   HKCR\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[threadingmodel]
                                   HKLM\software\microsoft\wbem\cimom[repository directory]
  Queries value:
  Queries value:
                                   HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[appid]
  Queries value:
                                   HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[dllsurrogate]
                                   HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[localservice]
  Oueries value:
  Queries value:
                                   HKCR \ | \ Table 1 - Table 2 - Tab
                                   HKCR\clsid\{7c857801-7381-11cf-884d-
  Oueries value:
00aa004b2e24}\inprocserver32[inprocserver32]
                                   HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[]
  Oueries value:
                                   HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[appid]
  Queries value:
                                  HKCR\clsid\{7c857801-7381-11cf-884d-
  Queries value:
00aa004b2e24}\inprocserver32[threadingmodel]
  Oueries value:
                                   HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32[]
                                   Queries value:
                                   HKCR\clsid\{d68af00a-29cb-43fa-8504-
  Oueries value:
ce99a996d9ea}\inprocserver32[inprocserver32]
                                   HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32[]
  Oueries value:
  Queries value:
                                   HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[appid]
  Queries value:
                                   HKCR\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[threadingmodel]
                                   HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
  Queries value:
                                   HKLM\software\microsoft\wbem\cimom[processid]
  Oueries value:
                                   HKLM\software\microsoft\wbem\cimom[enableprivateobjectheap]
  Queries value:
                                   HKLM\software\microsoft\wbem\cimom[contextlimit]
  Queries value:
                                   HKLM\software\microsoft\wbem\cimom[objectlimit]
                                   HKLM\software\microsoft\wbem\cimom[identifierlimit]
  Oueries value:
  Queries value:
                                   HKCR\interface\{027947e1-d731-11ce-a357-00000000001}\proxystubclsid32[]
  Queries value:
                                   HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[inprocserver32]
  Queries value:
                                   HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\tinprocserver32[]
                                   HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\[appid]
  Queries value:
                                   HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
  Oueries value:
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]
```

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

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

Value changes:

folders[cache]
Value changes:

folders[history]

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

folders[common appdata]

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

folders[appdata]

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

settings[proxyenable]

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

settings\connections[savedlegacysettings]

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

settings\zonemap[proxybypass]

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{\mathbb{N} internet.} \end{tabular}$ Value changes:

settings\zonemap[intranetname]

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

settings\zonemap[uncasintranet] Value changes:

HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap[autodetect]

Value changes:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints 2 \ \{f90255c2-6bc4-11e3-9fc7-16bc4-16$

806d6172696f}[baseclass]