Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3314, Task ID: 764

Task ID: 764 Risk Level: 10

Date Processed: 2016-05-18 10:35:40 (UTC)

Processing Time: 62.06 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\857bd61a8241ac81385ee957d8137887.exe"

Sample ID: 3314
Type: basic
Owner: admin

Label: 857bd61a8241ac81385ee957d8137887

 Date Added:
 2016-05-18 10:30:49 (UTC)

 File Type:
 PE32:win32:gui

File Type: PE32:win32:gui File Size: 184832 bytes

MD5: 857bd61a8241ac81385ee957d8137887

SHA256: efed61ac534b30cf6837dea448b72c43ec008f31273c445440a934aa5246ba2f

Description: None

Pattern Matching Results

3 HTTP connection - response code 200 (success)

5 Abnormal sleep detected

4 Checks whether debugger is present

10 Creates malicious events: Cycbot [Backdoor]

5 PE: Contains compressed section

3 Long sleep detected

Process/Thread Events

Creates process: C:\WINDOWS\Temp\857bd61a8241ac81385ee957d8137887.exe

["c:\windows\temp\857bd61a8241ac81385ee957d8137887.exe"]

Creates process: C:\WINDOWS\Temp\857bd61a8241ac81385ee957d8137887.exe

[c:\windows\temp\857bd61a8241ac81385ee957d8137887.exe startC:\Program

 $Files \verb|\LP\44D7\027.exe\%C: \verb|\Program Files\LP\44D7||$

Creates process: C:\WINDOWS\Temp\857bd61a8241ac81385ee957d8137887.exe [c:\windows\temp\857bd61a8241ac81385ee957d8137887.exe startC:\Documents and

 $Settings \land Admin \land Pplication \ Data \land TCD72 \land 19344.exe\%C: \land Documents \ and \ Settings \land Admin \land Application \ Data \land TCD72 \land 19344.exe\%C: \land Documents \ Admin \land Application \ Data \land TCD72 \land 19344.exe\%C: \land Documents \ Admin \land Application \ Data \land TCD72 \land 19344.exe\%C: \land Documents \ Admin \land Application \ Data \land TCD72 \land 19344.exe\%C: \land Documents \ Admin \land Application \ Data \land TCD72 \land 19344.exe\%C: \land Documents \ Data \land Documents \ Documents \ Data \land Documents \ Documents \ Data \land Documents \ Documents \ Documents \ Data \land Documents \ Document$

Data\7CD72]

Loads service: RASMAN [C:\WINDOWS\system32\svchost.exe -k netsvcs]
Terminates process: C:\WINDOWS\Temp\857bd61a8241ac81385ee957d8137887.exe

Named Object Events

 Creates mutex:
 \BaseNamedObjects\oleacc-msaa-loaded

 Creates mutex:
 \BaseNamedObjects\\5D92BB9F-9A66-458f-ACA4-66172A7016D4\}

 Creates mutex:
 \BaseNamedObjects\\4D92BB9F-9A66-458f-ACA4-66172A7016D4\}

 Creates mutex:
 \BaseNamedObjects\\61B98B86-5F44-42b3-BCA1-33904B067B81\}

 Creates mutex:
 \BaseNamedObjects\\816C7E24-B3B8-4962-BF5E-4B33FD2DFE78\}

 Creates mutex:
 \BaseNamedObjects\\61E0ECE180F-6E9E-4FA6-A154-6876D9DB8906\}

 Creates mutex:
 \BaseNamedObjects\\837C48AF-B05C-4520-8B38-2FE181D5DC78\}

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\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

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

1957994488-1003

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

1957994488-1003

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

1957994488-1003

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

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

507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003 Creates mutex: \BaseNamedObjects\4A3282FEF482C0F79E1

Creates event: \BaseNamedObjects\{6B985724-623F-492e-B0D6-C9715ADE853B}

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

Creates semaphore: \BaseNamedObjects\shell.{448F1A32-A340-11D1-BC6B-00A0C90312E1} \Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}

File System Events

Creates: C:\Program Files
Creates: C:\Program Files\72F66

Creates: C:\Documents and Settings\Admin\Application Data

```
C:\Documents and Settings\Admin\Application Data\7CD72
 Creates:
                         C:\Documents and Settings\Admin\Application Data\7CD72\2F66.CD7
 Creates:
 Creates:
                         C:\Program Files\LP
                         C:\Program Files\LP\44D7
 Creates:
 Opens:
                         C:\WINDOWS\Prefetch\857BD61A8241AC81385EE957D8137-17518D1E.pf
 Opens:
                         C:\Documents and Settings\Admin
                         C:\WINDOWS\system32\oleacc.dll
 Opens:
                         C:\WINDOWS\system32\msvcp60.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\msimg32.dll
                         C:\WINDOWS\system32\imm32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\oleaccrc.dll
 Opens:
                         C:\WINDOWS\system32\rasapi32.dll
 Opens:
                         C:\WINDOWS\system32\rasman.dll
 Opens:
                         C:\WINDOWS\system32\netapi32.dll
 Opens:
                         C:\WINDOWS\system32\ws2_32.dll
                         C:\WINDOWS\system32\ws2help.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\tapi32.dll
 Opens:
                         C:\WINDOWS\system32\rtutils.dll
 Opens:
                         C:\WINDOWS\system32\winmm.dll
                         C:\WINDOWS\system32\TAPI32.dll.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\TAPI32.dll.124.Config
 Opens:
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
 Opens:
                         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\shell32.dll
                         C:\WINDOWS\system32\SHELL32.dll.124.Manifest
 Opens:
 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:\WINDOWS\system32\winhttp.dll
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Config
 Opens:
                         C:\WINDOWS\system32\WININET.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\WININET.dll.123.Config
 Opens:
                         C:\
 Opens:
                         C:\Documents and Settings\Admin\Application Data\7CD72\2F66.CD7
                         C:\WINDOWS\system32\mswsock.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\dnsapi.dll
 Opens:
                         C:\WINDOWS\system32\iphlpapi.dll
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5
                         C:\Documents and Settings\Admin\Local Settings\History
 Opens:
 Opens:
                         C:\WINDOWS\Temp\857bd61a8241ac81385ee957d8137887.exe
                         C:\Documents and Settings\Admin\Local Settings\History\History.IE5
 Opens:
                         C:\WINDOWS\AppPatch\sysmain.sdb
 Opens:
 Opens:
                         C:\WINDOWS\AppPatch\systest.sdb
 Opens:
                         C:\WINDOWS\Temp
                         C:\WTNDOWS
 Opens:
 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
 Opens:
                         C:\windows\temp\857bd61a8241ac81385ee957d8137887.exe.Manifest
 Opens:
                         C:\WINDOWS\system32\drivers\etc\hosts
                         C:\WINDOWS\system32\rsaenh.dll
 Opens:
 Opens:
                         C:\AUTOEXEC.BAT
 Opens:
                         C:\Documents and Settings\All Users\Application
Data\Microsoft\Network\Connections\Pbk
                         C:\WINDOWS\system32\ras
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\Network\Connections\Pbk\
 Opens:
                         C:\WINDOWS\system32\sensapi.dll
                         C:\WINDOWS\system32\rpcss.dll
 Opens:
                         C:\WINDOWS\system32\MSCTF.dll
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Cloud AV 2012\ahst.lni
 Opens:
                         C:\WINDOWS\system32\clbcatq.dll
 Opens:
                         C:\WINDOWS\system32\comres.dll
 Opens:
                         C:\WINDOWS\Registration\R00000000007.clb
                         C:\WINDOWS\system32\msv1_0.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\crypt32.dll
 Opens:
 Opens:
                         C:\Program Files\LP\44D7\027.exe
                         C:\WINDOWS\system32\hnetcfg.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\wshtcpip.dll
                         C:\Documents and Settings\Admin\Application Data\Mozilla\
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Opera\
```

C:\WINDOWS\system32\rasadhlp.dll Opens: Opens: C:\WINDOWS\system32\winlogon.exe Opens: C:\WINDOWS\system32\xpsp2res.dll Opens: C:\WINDOWS\system32\wbem\wbemprox.dll Opens: C:\WINDOWS\system32\wbem\wbemcomn.dll Opens: C:\WINDOWS\system32\wbem\wbemsvc.dll Opens: C:\WINDOWS\system32\wbem\fastprox.dll Opens: C:\WINDOWS\system32\ntdsapi.dll Opens: C:\WINDOWS\system32\winrnr.dll

Opens:

Opens: C:\Documents and Settings

C:\Documents and Settings\Admin\Application Data Opens: Opens: C:\Documents and Settings\Admin\Application Data\7CD72

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

Opens: C:\WINDOWS\AppPatch C:\WINDOWS\Registration Opens: C:\WINDOWS\system32 Opens: Opens: C:\WINDOWS\system32\config Opens: C:\WINDOWS\system32\drivers Opens: C:\WINDOWS\system32\drivers\etc Opens: C:\WINDOWS\system32\wbem

C:\WINDOWS\WinSxS Opens:

Opens: C:\WINDOWS\system32\ntdll.dll Opens: C:\WINDOWS\system32\kernel32.dll Opens: C:\WINDOWS\SYSTEM32\CONFIG\SYSTEM Opens: C:\WINDOWS\system32\unicode.nls Opens: C:\WINDOWS\system32\locale.nls Opens: C:\WINDOWS\system32\sorttbls.nls C:\WINDOWS\system32\msvcrt.dll Opens: Opens: C:\WINDOWS\system32\user32.dll Opens: C:\WINDOWS\system32\gdi32.dll Opens: C:\WINDOWS\system32\advapi32.dll Opens: C:\WINDOWS\system32\rpcrt4.dll Opens: C:\WINDOWS\system32\secur32.dll Opens: C:\WINDOWS\system32\ole32.dll Opens: C:\WINDOWS\system32\oleaut32.dll Opens: C:\WINDOWS\system32\ctype.nls Opens: C:\WINDOWS\system32\sortkey.nls Opens: C:\WINDOWS\system32\apphelp.dll Opens: C:\WINDOWS\system32\shlwapi.dll C:\WINDOWS\system32\wininet.dll Opens: Opens: C:\WINDOWS\system32\normaliz.dll Opens: C:\WINDOWS\system32\urlmon.dll C:\WINDOWS\system32\iertutil.dll

C:\WINDOWS\system32\wldap32.dll Opens: C:\Documents Opens: C:\Documents and

C:\Documents and Settings\Admin\Application Opens:

C:\WINDOWS\system32\userenv.dll

C:\WINDOWS\system32\version.dll

Opens: C:\Documents and Settings\Admin\Application Data\7CD72\19344.exe Writes to: C:\Documents and Settings\Admin\Application Data\7CD72\2F66.CD7

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

Reads from: C:\AUTOEXEC.BAT

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

Reads from: C:\WINDOWS\Prefetch\857BD61A8241AC81385EE957D8137-17518D1E.pf

Network Events

Opens: Opens:

Opens:

Opens:

DNS query: istockanalyst.com DNS query: xprstats.com DNS query: hvw.dudlik-munik.com DNS query: 17k9g5fj.opalimanos.com DNS query: crl.verisign.com

DNS query: csc3-2009-2-crl.verisign.com DNS query: csc3-2010-crl.verisign.com DNS query: cdn.adventofdeception.com DNS query: h4159w.kupinosis.com DNS query: www.google.com complaintsboard.com DNS query: DNS query: e2iatwi.kupinosis.com

DNS query: highspeedinternetlosangeles.webnode.com DNS response: istockanalyst.com ⇒ 52.32.71.215 DNS response: hvw.dudlik-munik.com \Rightarrow 173.230.133.99 DNS response: e6845.dscb1.akamaiedge.net ⇒ 23.15.149.163

DNS response: www.google.com \Rightarrow 58.26.8.109 DNS response: www.google.com \Rightarrow 58.26.8.99 DNS response: www.google.com \Rightarrow 58.26.8.89 www.google.com \Rightarrow 58.26.8.94 DNS response: DNS response: www.google.com \Rightarrow 58.26.8.103 www.google.com \Rightarrow 58.26.8.98 DNS response:

DNS response: www.google.com \Rightarrow 58.26.8.108 www.google.com \Rightarrow 58.26.8.113 DNS response: DNS response: www.google.com \Rightarrow 58.26.8.84 www.google.com \Rightarrow 58.26.8.93 DNS response: DNS response: www.google.com \Rightarrow 58.26.8.119 DNS response: www.google.com \Rightarrow 58.26.8.118 DNS response: www.google.com \Rightarrow 58.26.8.104 www.google.com \Rightarrow 58.26.8.114 DNS response: DNS response: www.google.com \Rightarrow 58.26.8.123 www.google.com \Rightarrow 58.26.8.88 DNS response: complaintsboard.com \Rightarrow 50.31.101.62 DNS response:

DNS response: highspeedinternetlosangeles.webnode.com ⇒ 217.11.242.82

 Connects to:
 52.32.71.215:80

 Connects to:
 173.230.133.99:80

 Connects to:
 23.15.149.163:80

 Connects to:
 58.26.8.109:80

 Connects to:
 50.31.101.62:80

 Connects to:
 217.11.242.82:80

 Sends data to:
 8.8.8.8:53

 Sends data to:
 istockanalyst.com:80 (52.32.71.215)

 Sends data to:
 hvw.dudlik-munik.com:80 (173.230.133.99)

 Sends data to:
 e6845.dscb1.akamaiedge.net:80 (23.15.149.163)

Sends data to: 127.0.0.1:1048

Sends data to: www.google.com:80 (58.26.8.109)
Sends data to: complaintsboard.com:80 (50.31.101.62)

Sends data to: highspeedinternetlosangeles.webnode.com:80 (217.11.242.82)

Receives data from: 0.0.0.0:0

Receives data from: istockanalyst.com:80 (52.32.71.215)

Receives data from: 127.0.0.1:1048

Receives data from: e6845.dscb1.akamaiedge.net:80 (23.15.149.163)

Receives data from: www.google.com:80 (58.26.8.109)
Receives data from: complaintsboard.com:80 (50.31.101.62)

Receives data from: highspeedinternetlosangeles.webnode.com:80 (217.11.242.82)

Windows Registry Events

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

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

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

folders

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

 $\label{lem:condition} {\it Creates key:} \qquad \qquad {\it HKCU\software\microsoft\windows\currentversion\internet}$

settings\connections

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: HKLM\software\microsoft\wbem\cimom

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\857bd61a8241ac81385ee957d8137887.exe

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

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msvcrt.dll

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\gdi32.dll

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

options\user32.dll

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

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

options\imm32.dll

Opens key: $\mbox{HKLM} \mbox{ htcurrentversion} \mbox{ image file execution options $$ \mbox{ options $$ \mbox{ htdl1.dl1} $}$

Opens key: options\kernel32.dll

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

Opens key:

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

options\secur32.dll
 Opens key:

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

options\rpcrt4.dll
 Opens key:

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

options\advapi32.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ole32.dll

Opens kovi

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

```
options\oleaut32.dll
     Opens kev:
                                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleacc.dll
      Opens key:
                                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msimg32.dll
      Opens key:
                                                                                  HKLM\system\currentcontrolset\control\error message instrument\
                                                                                  HKLM\system\currentcontrolset\control\error message instrument
      Opens key:
                                                                                  HKLM\software\microsoft\windows nt\currentversion\gre_initialize
      Opens key:
                                                                                  HKLM\software\microsoft\windows nt\currentversion\compatibility32
      Opens key:
      Opens key:
                                                                                  HKLM\software\microsoft\windows nt\currentversion\ime compatibility
      Opens key:
                                                                                  HKLM\software\microsoft\windows nt\currentversion\windows
      Opens key:
                                                                                  \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + nt + current + version + winlog on + current + version + version
      Opens key:
                                                                                  HKLM\
                                                                                 \label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} icrosoft \end{tabular} windows nt \current version \end{tabular} diagnostics
      Opens key:
      Opens key:
                                                                                  HKLM\software\microsoft\ole
      Opens key:
                                                                                  HKCR\interface
                                                                                 HKCR\interface\{00020400-0000-0000-c000-00000000046}
      Opens kev:
      Opens key:
                                                                                  HKLM\software\microsoft\oleaut
      Opens key:
                                                                                  HKLM\software\microsoft\oleaut\userera
      Opens key:
                                                                                 HKCU\
      Opens key:
                                                                                  HKCU\software\policies\microsoft\control panel\desktop
      Opens key:
                                                                                  HKCU\control panel\desktop
                                                                                  HKLM\software\microsoft\active accessibility\handlers
      Opens key:
      Opens key:
                                                                                  HKCU\software\classes\
      Opens key:
                                                                                  HKCU\software\classes\typelib
      Opens key:
                                                                                  HKCR\typelib
      Opens key:
                                                                                  HKCU \setminus software \setminus classes \setminus typelib \setminus \{1ea4dbf0-3c3b-11cf-810c-00aa00389b71\}
                                                                                  HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}
      Opens key:
                                                                                  \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \typelib \floor= 1.1 cf-810c-00aa00389b71 \classes \class
      Opens key:
      Opens key:
                                                                                  HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1
      Opens key:
                                                                                  HKCU\software\classes\typelib\{1ea4dbf0-3c3b-11cf-810c-
 00aa00389b71}\1.1\flags
      Opens key:
                                                                                  HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1\flags
      Opens key:
                                                                                  HKCU\software\classes\typelib\{1ea4dbf0-3c3b-11cf-810c-
00aa00389b71}\1.1\0
      Opens key:
                                                                                  HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1\0
      Opens key:
                                                                                  HKCU\software\classes\typelib\{1ea4dbf0-3c3b-11cf-810c-
00aa00389b71}\1.1\0\win32
      Opens key:
                                                                                  HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1\0\win32
      Opens key:
                                                                                 HKCU\software\classes\typelib\{1ea4dbf0-3c3b-11cf-810c-
00aa00389b71}\1.1\helpdir
      Opens key:
                                                                                  \label{lem:hkcr-typelib-flead} $$ HKCR \typelib {1ea4dbf0-3c3b-11cf-810c-00aa00389b71} \1.1 \end{typelib} $$ $$ help directly $$ help direct
      Opens key:
                                                                                  HKCU\software\classes\interface
                                                                                  HKCU\software\classes\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}
      Opens key:
      Opens key:
                                                                                  HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}
      Opens key:
                                                                                 HKCU\software\classes\interface\{618736e0-3c3d-11cf-810c-
00aa00389b71}\proxystubclsid
      Opens key:
                                                                                  HKCR \verb|\| face \verb|\| \{618736e0-3c3d-11cf-810c-00aa00389b71\} \verb|\| proxystubclsid| 
                                                                                  HKCU\software\classes\interface\{618736e0-3c3d-11cf-810c-
      Opens kev:
 00aa00389b71}\proxystubclsid32
                                                                                  HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid32
      Opens key:
      Opens key:
                                                                                  HKCU\software\classes\interface\{618736e0-3c3d-11cf-810c-
00aa00389b71}\typelib
      Opens key:
                                                                                  HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\typelib
      Opens kev:
                                                                                  HKCU\software\classes\interface\{03022430-abc4-11d0-bde2-00aa001a1953}
                                                                                  HKCR\interface\{03022430-abc4-11d0-bde2-00aa001a1953}
      Opens key:
                                                                                  HKCU\software\classes\interface\{03022430-abc4-11d0-bde2-
      Opens key:
00aa001a1953}\proxystubclsid
                                                                                  HKCR \verb|\| interface \verb|\| \{03022430-abc4-11d0-bde2-00aa001a1953\} \verb|\| | proxystubclsid| | the content of the c
      Opens key:
      Opens key:
                                                                                  HKCU\software\classes\interface\{03022430-abc4-11d0-bde2-
 00aa001a1953}\proxystubclsid32
                                                                                 HKCR \setminus \{03022430-abc4-11d0-bde2-00aa001a1953\} \setminus proxystubclsid32
      Opens key:
      Opens key:
                                                                                  HKCU \setminus software \setminus classes \setminus interface \setminus \{03022430 - abc4 - 11d0 - bde2 - abc4 - abc4
00aa001a1953}\typelib
      Opens key:
                                                                                  HKCR\interface\{03022430-abc4-11d0-bde2-00aa001a1953}\typelib
      Opens key:
                                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\apphelp.dll
                                                                                  \label{lem:hklm} \verb+Kklm/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\ws2help.dll
      Opens key:
                                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.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\shlwapi.dll
      Opens key:
                                                                                  HKLM\software\microsoft\windows\currentversion\explorer\performance
      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:
Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\tapi32.dll
 Opens kev:
Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
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\rasapi32.dll
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\telephony
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shell32.dll
 Opens key:
                         HKLM\system\setup
 Opens kev:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winhttp.dll
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\internet
settings\winhttp\tracing
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\normaliz.dll
 Opens kev:
                         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:
                         HKCU\software\classes\protocols\name-space handler\
 Opens key:
                         HKCR\protocols\name-space handler
 Opens key:
                         HKCU\software\classes\protocols\name-space handler
 Opens key:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings
                         HKLM\software\microsoft\windows\currentversion\internet settings
 Opens key:
 Opens key:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings
                        HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_protocol_lockdown
                        HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_protocol_lockdown
 Opens key:
                        HKLM\software\policies\microsoft\windows\currentversion\internet
settings\
                        \label{lem:hklmsoftware policies microsoft internet explorer \verb|\main| feature control| \\
 Opens key:
 Opens key:
                         \label{lem:hkcu} \verb+KKCU\software\policies\microsoft\internet\ explorer\main\feature control
                         HKLM\software\microsoft\internet explorer\main\featurecontrol
 Opens kev:
                        HKCU\software\microsoft\internet explorer\main\featurecontrol
 Opens key:
                         HKCU\software\microsoft\internet
 Opens kev:
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 kev:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zonemap\domains\
 Opens key:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
 Opens key:
                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
                        HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_unc_savedfilecheck
 Opens key:
                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wininet.dll
 Opens key:
                         HKLM\system\currentcontrolset\control\wmi\security
 Opens key:
                         HKCU\software\microsoft\windows nt\currentversion\windows
 Opens key:
                        HKLM\software\microsoft\rpc\pagedbuffers
 Opens key:
                         HKLM\software\microsoft\rpc
 Opens key:
                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\857bd61a8241ac81385ee957d8137887.exe\rpcthreadpoolthrottle
 Opens key:
                        HKLM\software\policies\microsoft\windows nt\rpc
 Opens kev:
                         HKLM\software\microsoft\windows\currentversion
 Opens key:
                        HKLM\system\currentcontrolset\services\winsock2\parameters
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
 Opens kev:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001
 Opens key:
```

Opens kev:

Opens key:

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

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

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

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

Opens key:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \namespace_catalog 5 \00000004 \normalfooth Gpens key:$

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

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

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

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\dnsapi.dll

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

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

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

Opens key: HKLM\software
Opens key: HKLM\software
Opens key: HKLM\software\pa

Opens key: HKLM\software\policies\microsoft\internet explorer
Opens key: HKLM\software\policies\microsoft\internet explorer\main
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key: HKLM\software\microsoft\windows\currentversion\internet

settings\5.0\cache

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

settings\5.0\cache

Opens key: $\label{local-opens} \mbox{HKCU\software\microsoft\windows\currentversion\internet} \\$

settings\5.0\cache\content
Opens kev:

H

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

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

Opens key: options\iphlpapi.dll

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

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

Opens key: HKLM\system\currentcontrolset\services\netbt\parameters
Opens key: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\cookies

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

settings\5.0\cache\cookies

Opens key:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-4404, and the services \ tcpip \ parameters \ terfaces \ terf$

c7d49d7cecdc}

Opens key: $\label{local-opens} \mbox{HKCU\software\microsoft\windows\currentversion\internet} \\$

settings\5.0\cache\history

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

settings\5.0\cache\history

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

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

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

Opens key: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags\custom\857bd61a8241ac81385ee957d8137887.exe

Opens key: HKLM\software\policies\microsoft\windows\safer\levelobjects

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

Opens key:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus a3f824 - d8cb - 441b - 834d - d8cb -$

be2efd2c1a33}

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

 $\label{thm:linear_control} Opens key: $$ HKLM\system\currentcontrolset\control\computername active computername $$ Opens key: $$ HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes $$ Ohashes $$ Oha$

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89edd5fbde1328} Opens key: b813f72dbb91} Opens key: $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0\ hashes \ \{81d1fe15-dd9d-4762-b16d$ 7c29ddecae3f} Opens key: 085bcc18a68d} Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache $\label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+$ Opens key: settings\5.0\cache\extensible cache\domstore Opens kev: $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe$ b91490411bfc} Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths Opens key: HKLM\software\policies\microsoft\system\dnsclient $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Opens key: settings\5.0\cache\extensible cache\feedplat Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes Opens kev: $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus urlzones$ Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes Opens key: Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Opens key: settings\5.0\cache\extensible cache\iecompat Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths Opens kev: Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes Opens key: $\label{thm:local_hammon_hammon} HKCU \software \policies \microsoft \windows \safer \code identifiers \normalised \partial \normalised \partial \$ 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: 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 HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\extensible cache\ietld Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012014033120140407 Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths Opens kev: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths

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

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

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

Opens kev:

Opens key:

Opens key:

settings\5.0\cache\extensible cache\mshist012014041220140413 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\cache\extensible cache\privacie: Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset HKCU\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_bufferbreaking_818408 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_bufferbreaking_818408 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954 HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\5.0\cache Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\5.0\cache HKCU\software\microsoft\internet Opens kev: 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 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149 HKLM\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_allow_long_international_filenames Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_allow_long_international_filenames HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274 Opens kev: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback HKLM\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_disallow_null_in_response_headers Opens kev: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_disallow_null_in_response_headers HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_digest_no_extras_in_uri Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_digest_no_extras_in_uri HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615 HKLM\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615 Opens key: Opens key: HKLM\software\microsoft\tracing\rasapi32 Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$ options\userenv.dll HKLM\system\currentcontrolset\control\productoptions Opens kev: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders Opens key: HKLM\software\policies\microsoft\windows\system Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist Opens key: HKLM\system\currentcontrolset\control\session manager\environment

Opens key: HKCU\volatile environment Opens key: options\sensapi.dll

HKCU\environment

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

 $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus profile list \setminus s-1-5-21-1 = (a. 1) + (b. 1) +$

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

options\msctf.dll

1757981266-507921405-1957994488-1003

Opens kev:

Opens key:

Opens key:

HKLM\software\microsoft\ctf\compatibility\857bd61a8241ac81385ee957d8137887.exe

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

Opens key: Opens key: HKCU\keyboard layout\toggle

Opens key: HKLM\software\microsoft\ctf\ Opens key: HKLM\system\currentcontrolset\control\securityproviders HKLM\system\currentcontrolset\control\lsa\sspicache Opens key:

HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll Opens key: Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll

Opens key: HKLM\software\microsoft\com3

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

options\comres.dll

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

options\version.dll

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

options\clbcatq.dll

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

Opens key: HKLM\software\classes

 $\label{lem:hklm} \verb+Kklm \+ system \+ control \+ lsa \+ spicache \+ msnsspc.dll$ Opens key:

Opens key: HKCR\clsid

Opens key: HKLM\system\currentcontrolset\control\securityproviders\saslprofiles HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4} Opens kev:

Opens key: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4} Opens key: HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-

b913c40c9cd4}\treatas

Opens key: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\treatas Opens key: HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-

b913c40c9cd4}\inprocserver32

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

options\msv1_0.dll

HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-

b913c40c9cd4}\inprocserverx86

Opens key: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-

b913c40c9cd4}\localserver32

HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\localserver32 Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rsaenh.dll

HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-Opens key:

b913c40c9cd4}\inprochandler32

Opens key: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler32

HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-Opens key:

b913c40c9cd4}\inprochandlerx86

HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandlerx86 Opens key:

HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-Opens key:

b913c40c9cd4}\localserver

HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\localserver Opens kev:

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

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

options\hnetcfg.dll

HKLM\software\microsoft\cryptography Opens key: Opens key: HKLM\software\microsoft\cryptography\offload

Opens kev:

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

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

options\wshtcpip.dll

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

options\rasadhlp.dll

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

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

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

00aa004b2e24}\inprocserver32

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

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

00aa004b2e24}\inprocserverx86

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

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

00aa004b2e24}\localserver32

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

00aa004b2e24}\inprochandler32

Opens key:

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

00aa004b2e24}\inprochandlerx86

Opens key:

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

00aa004b2e24}\localserver

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

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

options\wbemcomn.dll

Opens key:

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

options\wbemprox.dll

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

options\xpsp2res.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

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

00c04fb68820}\inprocserver32

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

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

00c04fb68820}\inprocserverx86

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

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

00c04fb68820}\localserver32

HKCR\clsid\{8hc3f05e-d86h-11d0-a075-00c04fh68820}\localserver32 Opens kev:

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

00c04fb68820}\inprochandler32

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

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

00c04fb68820}\inprochandlerx86

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

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

00c04fb68820}\localserver

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

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

 $\label{local-eq:hkcu} \begin{tabular}{ll} HKCU \software \classes \interface \ \{f309ad18-d86a-11d0-a075-00c04fb68820\} \end{tabular}$ Opens key:

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

00c04fb68820}\proxystubclsid32

Opens key: $HKCR \land f309 ad 18-d86 a-11 d0-a075-00 c04 fb68820 \rbrace \land proxystubclsid 32$ Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}

HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24} Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{7c857801-7381-11cf-884d-146844-14684404-146844-146844-14684-1468444-146844-14684-14684-14684-14684-14684-14684-14684-14684-14684-$

00aa004b2e24}\treatas

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

00aa004b2e24}\inprocserver32

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

Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{7c857801-7381-11cf-884d-146844-14684404-146844-146844-14684-1468444-146844-14684-14684-14684-14684-14684-14684-14684-14684-14684-$

00aa004b2e24}\inprocserverx86

Opens key:

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

00aa004b2e24}\localserver32

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

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

00aa004b2e24}\inprochandler32

 $\label{lem:hkcr} $$ HKCR\clsid\\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler 32 $$ $$$ Opens key:

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

00aa004b2e24}\inprochandlerx86

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

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

00aa004b2e24}\localserver

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

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

options\wbemsvc.dll

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

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

930efe48a887}\proxystubclsid32

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

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

00aa003240c7}\proxystubclsid32

 $HKCR \verb|\interface| \{9556dc99-828c-11cf-a37e-00aa003240c7\} \verb|\proxystubclsid32|$ Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{d68af00a-29cb-43fa-8504-ce99a996d9ea\}$

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

ce99a996d9ea}\treatas

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

ce99a996d9ea}\inprocserver32

HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32 Opens kev:

Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504ce99a996d9ea}\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}\localserver32

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\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: HKLM\software\microsoft\wbem\cimom

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

Opens key: HKCR\interface\{027947e1-d731-11ce-a357-000000000011}
Opens key: HKCU\software\classes\interface\{027947e1-d731-11ce-a357-

00000000001}\proxystubclsid32

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

 $\label{lem:continuous} Opens key: $$ HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}$$ Opens key: $$ HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-0014b703efd}$$$

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

 $Opens~key: \\ HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler 32$

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

 $00104b703efd \verb|\inprochandlerx86| \\$

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

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

00104b703efd}\localserver

Opens key: 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: 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

Opens key: HKLM\software\microsoft\windows defender

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

options\winrnr.dll

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

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

Queries value:

 $\label{lem:hklm} \verb+Kklm/software\policies/microsoft/windows/safer/code identifiers[transparentenabled]$

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

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

Queries value: HKLM\software\microsoft\windows

nt\currentversion\compatibility32[857bd61a8241ac81385ee957d8137887]

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

compatibility[857bd61a8241ac81385ee957d8137887]

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

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

manager[criticalsectiontimeout]

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

Queries value: HKCR\interface[interfacehelperdisableall]

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

```
HKCR\interface\{00020400-0000-0000-c000-
  Oueries value:
00000000046}[interfacehelperdisableall]
                                   HKCR\interface\{00020400-0000-0000-c000-
  Oueries value:
00000000046}[interfacehelperdisableallforole32]
                                   HKCU\control panel\desktop[multiuilanguageid]
  Oueries value:
  Queries value:
                                   manager[safeprocesssearchmode]
                                   HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1[]
  Oueries value:
  Oueries value:
                                   HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1\flags[]
  Oueries value:
                                   HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1\0\win32[]
                                   HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}[]
  Oueries value:
  Queries value:
                                   HKCR \ interface \ \{618736e0-3c3d-11cf-810c-00aa00389b71\} \ proxystubclsid[]
  Oueries value:
                                   HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid32[]
                                   HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\typelib[]
  Oueries value:
  Oueries value:
                                   HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\typelib[version]
  Oueries value:
                                   HKCR\interface\{03022430-abc4-11d0-bde2-00aa001a1953}[]
                                   HKCR \ | \ HKCR \ | 
  Oueries value:
  Queries value:
                                   HKCR\interface\{03022430-abc4-11d0-bde2-00aa001a1953}\proxystubclsid32[]
  Oueries value:
                                   HKCR\interface\{03022430-abc4-11d0-bde2-00aa001a1953}\typelib[]
                                   Oueries value:
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
  Oueries value:
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
  Oueries value:
  Queries 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]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
  Oueries value:
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
  Queries value:
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
  Queries value:
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
  Queries value:
  Oueries value:
                                   HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [aux 6]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
  Oueries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer51
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
  Queries value:
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
                                   HKCU\control panel\desktop[smoothscroll]
  Queries value:
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
HKLM\software\microsoft\windows\currentversion\telephony[tapi32maxnumrequestretries]
  Oueries value:
```

HKLM\system\setup[systemsetupinprogress] Oueries value:

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

settings[disableimprovedzonecheck]

HKLM\software\microsoft\internet Oueries value:

explorer\main\featurecontrol\feature_protocol_lockdown[857bd61a8241ac81385ee957d8137887.exe]

Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature protocol lockdown[*]

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

ab78-1084642581fb]

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

0000-0000000000000]

Queries value: HKLM\software\microsoft\rpc[maxrpcsize]

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

- HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
 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\000000000004[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem] Queries 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\000000000010[packedcatalogitem]
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
 Oueries value:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 0000000000001 \ [providerid] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Queries 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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
- 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
 Oueries value:
- $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws 2_32 numhandle buckets]$

```
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [prioritize record data]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[fromcachetimeout]
                         \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
 Queries value:
settings[secureprotocols]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
                         HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
 Queries value:
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
                         HKLM\software\policies\microsoft\internet
explorer\main[security_hklm_only]
 Oueries value:
                         HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablepassport]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[idnenabled]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[enablehttp1_1]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablebasicoverclearchannel]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
 Queries value:
Queries value:
```

```
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
  Queries 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[updatetopleveldomainzones]
                                    HKCU\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
  Queries value:
                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[clientauthbuiltinui]
                                    HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
  Queries value:
  Queries value:
                                    HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
                                    HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
  Oueries value:
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[syncmode5]
  Queries value:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache[signature]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\content[peruseritem]
  Queries value:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
                                    HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Oueries value:
folders[cache]
  Oueries value:
                                    HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cacheprefix]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cachelimit]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
                                    HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\cookies[peruseritem]
                                    HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Queries value:
folders[cookies]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
  Oueries value:
c7d49d7cecdc}[enabledhcp]
  Queries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-4404, and the services \ tcpip \ parameters \ terfaces \ terf
c7d49d7cecdc}[leaseobtainedtime]
  Oueries value:
c7d49d7cecdc}[leaseterminatestime]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpserver]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\cookies[cachelimit]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
  Queries value:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
```

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

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

manager\appcompatibility[disableappcompat]

Queries value: HKLM\system\wpa\mediacenter[installed]

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

settings\5.0\cache\history[cacheprefix]

Queries value:

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

Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]

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

settings\5.0\cache\history[cachelimit]

Queries value:

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

Queries value:

 $HKLM software \\policies \\microsoft \\windows \\safer \\code identifiers \\0 \\paths \\dda \\3f824-d8cb-441b-834d-be2efd \\2c1a \\3\\fitem \\data]$

Queries value:

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

Queries value:

Oueries value:

Queries value:

Oueries value:

Queries value:

Queries value:

 $HKLM software \\policies \\microsoft \\windows \\safer \\code identifiers \\0 \\hashes \\\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91\} \\label{eq:microsoft} \\hashelg \\1$

Queries value:

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{7fb9cd2e-3076-4df9-a57b-b813f72dbb91\} \ [saferflags]$

Queries value:

Queries value:

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \software \policies \microsoft \windows \safer \code identifiers \one \noise \park \noise \no$

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

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

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

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

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

 $settings \verb|\5.0| cache \verb|\extensible| cache \verb|\domstore[cacheprefix]|$

Queries value:

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

Queries value:

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

Queries value

 $\label{thm:hklm} HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{94e3e076-8f53-42a5-8411-085bcc18a68d \ rafer flags \ rafer \ fl$

Queries value:

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

Queries value

 $\label{local-equation} HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}\ [hashalg]$

Queries value:

 $HKLM software \verb|\policies| itemsize| MKLM software \verb|\policies| itemsize| dc971ee5-44eb-4fe4-ae2e-b91490411bfc \verb|\policies| dc971ee5-44eb-4fe4-ae2e-b91490411bfc \| dc971ee5-44eb-4fe4-ae2e-b9149041bfc \| dc971ee5-44e$

b91490411bfc}[saferflags] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\cache\extensible cache\domstore[cachelimit] Queries value: HKCU\software\microsoft\windows\currentversion\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] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat[cachepath] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\cache\extensible cache\feedplat[cacheprefix] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[queryadaptername] Oueries value: c7d49d7cecdc}[disableadapterdomainname] Oueries value: $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4300-abe3-4300-a$ c7d49d7cecdc}[registrationenabled] Oueries value: c7d49d7cecdc}[registeradaptername] Queries value: c7d49d7cecdc}[registrationmaxaddresscount] Oueries value: c7d49d7cecdc}[maxnumberofaddressestoregister] Queries value: c7d49d7cecdc}[domain] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[dhcpdomain] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\cache\extensible cache\feedplat[cachelimit] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\cache\extensible cache\feedplat[cacheoptions] HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\iecompat[cacherepair] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\iecompat[cachepath] HKCU\software\microsoft\windows\currentversion\internet 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] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\iecompat[cacheoptions] HKCU\software\microsoft\windows\currentversion\internet Oueries value: 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 Queries value: settings\5.0\cache\extensible cache\ietld[cacheprefix] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\cache\extensible cache\ietld[cachelimit] HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\ietld[cacheoptions] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel] c7d49d7cecdc}[ipautoconfigurationenabled] Queries value: $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4300-abe3-4300-a$ c7d49d7cecdc}[addresstype] c7d49d7cecdc}[nameserver] Queries value: $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4300-abe3-4300-a$ c7d49d7cecdc}[dhcpnameserver] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath] Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]

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

```
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
  Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
                           HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
  Queries value:
cryptographic provider[type]
  Queries value:
                           HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
                           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]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disableworkerthreadhibernation]
  Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablereadrange]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[keepalivetimeout]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
  Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
  Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[maxconnectionsper1_0server]
  Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[serverinfotimeout]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
                           HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[connecttimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[connectretries]
  Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[connectretries]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[sendtimeout]
                           HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[sendtimeout]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
                           HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[receivetimeout]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[certcachenovalidate]
```

```
Oueries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                             HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelimit]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[httpdefaultexpirytimesecs]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
                             HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[857bd61a8241ac81385ee957d8137887.exe]
                             HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature disable unicode handle closing callback[*]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[perusercookies]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[leashlegacycookies]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablent4rascheck]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dialupuselansettings]
                             HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dialupuselansettings]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendextracrlf]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypassftptimecheck]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[releasesocketduringauth]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[releasesocketduring401auth]
 Oueries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[wpadsearchalldomains]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablelegacypreauthasserver]
 Queries value:
                             \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
settings[disablelegacypreauthasserver]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasshttpnocachecheck]
 Oueries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
 Oueries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
 Oueries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
                             HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[nocheckautodialoverride]
 Oueries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
 Queries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                             HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sharecredswithwinhttp]
 Queries value:
                             \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[mimeexclusionlistforcache]
 Queries value:
                             \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[headerexclusionlistforcache]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dnscacheenabled]
 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[dnscacheentries]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonpost]
 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[warnalwaysonpost]
 Queries value:
                             \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings[warnonzonecrossing]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonbadcertsending]
 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}.
```

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

settings[warnonbadcertrecving]

```
settings[warnonpostredirect]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[alwaysdrainonredirect]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
  Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
settings[globaluseroffline]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[enableautodial]
  Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[urlencoding]
  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[truncatefilename]
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
 Oueries value:
settings[badproxyexpirestime]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries 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
  Queries value:
settings\connections[savedlegacysettings]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\connections[defaultconnectionsettings]
                            HKLM\software\microsoft\tracing[enableconsoletracing]
  Queries value:
  Queries value:
                            HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
                            HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
  Queries value:
                            HKLM \verb|\software\microsoft\tracing\rasapi32[enable consolet racing]|
  Queries value:
  Queries value:
                            HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
  Oueries value:
                            HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
                            HKLM\software\microsoft\tracing\rasapi32[filedirectory]
  Queries value:
                            HKLM\software\microsoft\windows\currentversion\explorer\user shell
  Oueries value:
folders[common appdata]
                            HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\winlogon[userenvdebuglevel]
                           HKLM\software\microsoft\windows
  Oueries value:
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
  Queries value:
folders[local settings]
  Queries value:
                            HKLM\software\microsoft\windows
nt\currentversion\winlogon[rsopdebuglevel]
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
                           HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\profilelist[profilesdirectory]
  Queries value:
                           HKLM\software\microsoft\windows
nt\currentversion\profilelist[allusersprofile]
  Oueries value:
                           HKLM\software\microsoft\windows
nt\currentversion\profilelist[defaultuserprofile]
  Queries value:
                           HKLM\software\microsoft\windows\currentversion[commonfilesdir]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[profileimagepath]
                           HKCU\software\microsoft\windows
  Queries value:
nt\currentversion\winlogon[parseautoexec]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
                            HKLM\software\microsoft\ctf\systemshared[cuas]
  Oueries value:
  Queries value:
                            HKLM\software\microsoft\rpc\securityservice[10]
                            HKCU\keyboard layout\toggle[language hotkey]
  Oueries value:
  Queries value:
                            HKCU\keyboard layout\toggle[hotkey]
  Oueries value:
                            HKCU\keyboard layout\toggle[layout hotkey]
  Queries value:
                            HKLM\software\microsoft\ctf[enableanchorcontext]
  Oueries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
                            HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
  Oueries value:
  Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]
  Queries value:
                           HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]
  Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[version]
  Oueries value:
                           HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]
  Queries value:
                            HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]
```

```
HKLM\software\microsoft\com3[com+enabled]
  Oueries value:
                                   HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
  Oueries value:
                                   {\tt HKLM \setminus software \setminus microsoft \setminus ole[minimumfreemempercentage to create object]}
  Oueries value:
                                   HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]
  Queries value:
  Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities]
                                   HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version]
  Oueries value:
                                   Oueries value:
  Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize]
                                  HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name]
  Queries value:
  Oueries value:
                                   HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment]
  Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities]
                                   HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid]
  Queries value:
  Oueries value:
                                   HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version]
  Queries value:
                                   HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize]
  Queries value:
                                  HKLM\software\microsoft\com3[regdbversion]
                                   HKCR\clsid\{304ce942-6e39-40d8-943a-
  Queries value:
b913c40c9cd4}\inprocserver32[inprocserver32]
  Queries value:
                                  HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32[]
  Oueries value:
                                  HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}[appid]
                                  HKCR\clsid\{304ce942-6e39-40d8-943a-
  Oueries value:
b913c40c9cd4}\inprocserver32[threadingmodel]
  Queries value:
                                  HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
                                  HKLM\software\microsoft\cryptography[machineguid]
  Oueries value:
  Queries value:
                                   HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Queries value:
                                  HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  Queries value:
Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [helperdllname]
                                   HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
  Queries value:
  Queries value:
                                   HKLM\software\microsoft\ole[maximumallowedallocationsize]
                                  {\tt HKLM \ } system \verb|\ current control \ \\ lsa[every one includes an ony mous]
  Oueries value:
                                  HKCR\clsid\{4590f811-1d3a-11d0-891f-
  Oueries value:
00aa004b2e24}\inprocserver32[inprocserver32]
                                  \label{local-bound} \begin{tabular}{ll} HKCR\clsid & \{4590f811-1d3a-11d0-891f-00aa004b2e24\} \label{local-bound} \end{tabular} $$ in processing the context of the context
  Oueries value:
  Queries value:
                                   HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[appid]
  Queries value:
                                  HKCR\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[threadingmodel]
                                  HKLM\software\microsoft\wbem\cimom[logging directory]
  Oueries value:
                                   HKLM\software\microsoft\wbem\cimom[logging]
  Queries value:
  Oueries value:
                                   HKLM\software\microsoft\wbem\cimom[log file max size]
  Queries value:
                                   HKLM\software\microsoft\wbem\cimom[repository directory]
  Oueries value:
                                   HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[appid]
                                   HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[dllsurrogate]
  Queries value:
                                   HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[localservice]
  Oueries value:
  Queries value:
                                   HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32[]
                                  HKCR\clsid\{7c857801-7381-11cf-884d-
  Oueries value:
00aa004b2e24}\inprocserver32[inprocserver32]
  Queries value:
                                  HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[]
                                  HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[appid]
  Oueries value:
  Queries value:
                                  HKCR\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[threadingmodel]
                                  HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32[]
  Oueries value:
  Queries value:
                                   HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32[]
  Queries value:
                                  HKCR\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[inprocserver32]
  Queries value:
                                  HKCR \c1sid \d68af00a-29cb-43fa-8504-ce99a996d9ea \nprocserver 32[]
  Queries value:
                                  HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[appid]
                                  HKCR\clsid\{d68af00a-29cb-43fa-8504-
  Queries value:
ce99a996d9ea}\inprocserver32[threadingmodel]
  Oueries value:
                                  HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
  Oueries value:
                                   HKLM\software\microsoft\wbem\cimom[processid]
  Queries 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:
  Oueries value:
                                   HKCR\interface\{027947e1-d731-11ce-a357-00000000001}\proxystubclsid32[]
  Oueries value:
                                  HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[inprocserver32]
                                  HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32[]
  Oueries value:
```

Queries value: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprocserver32[threadingmodel]

Queries value: HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}\proxystubclsid32[]
Queries value: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32[]

Queries value: HKLM\system\currentcontrolset\services\netbt\linkage[export]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet

settings[proxyserver]

Value changes: HKLM\software\microsoft\cryptography\rng[seed]

Value changes: HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1\0\win32[] Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[cache]

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

folders[cookies]

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

folders[history]
Value changes:

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

settings\connections[defaultconnectionsettings]

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

settings[proxyenable]

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

settings\connections[savedlegacysettings]

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

settings[proxyserver]