Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details Host: mag2, Sample ID: 3308, Task ID: 740

Task ID: 740

Risk Level:

Date Processed: 2016-05-18 10:32:33 (UTC)

Processing Time: 61.38 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\6bb534e6c0348b33b54c16dff868e84d.exe"

3308 Sample ID: Type: Owner: basic admin

6bb534e6c0348b33b54c16dff868e84d Label:

2016-05-18 10:30:48 (UTC) Date Added: File Type: PE32:win32:gui:.net

53760 bytes File Size: MD5:

6bb534e6c0348b33b54c16dff868e84d b2b97a02e614803454ab41f62b1d21e177f742cdc9d280c1712f0c0d7d89394c SHA256:

Description:

Pattern Matching Results

2 .NET compiled executable

YARA score 7

Writes to a log file [Info]

4 Reads process memory

Static Events

YARA rule hit: NET_Obfuscation

Process/Thread Events

C:\WINDOWS\Temp\6bb534e6c0348b33b54c16dff868e84d.exe Creates process:

["c:\windows\temp\6bb534e6c0348b33b54c16dff868e84d.exe"]

Creates process: C:\PROGRA~1\COMMON~1\MICROS~1\DW\DW20.EXE [dw20.exe -x -s 296]

Loads service: RASMAN [C:\WINDOWS\system32\svchost.exe -k netsvcs]

Reads from process: PID:1652 C:\WINDOWS\Temp\6bb534e6c0348b33b54c16dff868e84d.exe

Named Object Events

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

1957994488-1003 Creates mutex:

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

1957994488-1003

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

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

1957994488-1003

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

\BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-Creates mutex: 507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003

Creates mutex: \BaseNamedObjects\oleacc-msaa-loaded

Creates mutex: $\verb|\BaseNamedObjects|| c: !documents and settings! admin! local|$

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 event: \BaseNamedObjects\CorDBIPCSetupSyncEvent_1652

Creates event: \BaseNamedObjects\MsoDWHang6741108160

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

\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1} Creates semaphore: Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}

Creates semaphore: \BaseNamedObjects\MsoDWExclusive1652

File System Events

Creates C:\Documents and Settings\Admin\Local Settings\Temp\dw.log Creates: C:\Documents and Settings\Admin\Local Settings\Temp\A5E762.dmp C:\WINDOWS\Prefetch\6BB534E6C0348B33B54C16DFF868E-37663D9B.pf Opens:

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

C:\windows\temp\6bb534e6c0348b33b54c16dff868e84d.exe.config Opens: C:\WINDOWS\Temp\6bb534e6c0348b33b54c16dff868e84d.exe Opens:

C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727 Opens: Opens:

C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll.2.Manifest Opens: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll.2.Config Opens:

Opens:

C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-ww_b80fa8ca Opens:

C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-

ww_b80fa8ca\msvcr80.dll

Opens: C:\WINDOWS Opens:

C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config Opens: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\security.config Opens: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch Opens:

```
Opens:
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config
Opens:
                                                 C:\WINDOWS\system32\shell32.dll
   Opens:
                                                 C:\WINDOWS\system32\shell32.dll.124.Manifest
   Opens:
                                                 C:\WINDOWS\system32\shell32.dll.124.Config
   Opens:
                                                 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
                                                 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
                                                 C:\WINDOWS\WindowsShell.Manifest
   Opens:
   Opens:
                                                 C:\WINDOWS\WindowsShell.Config
                                                 C:\WINDOWS\system32\comctl32.dll
   Opens:
                                                 C:\WINDOWS\system32\comctl32.dll.124.Manifest
   Opens:
   Opens:
                                                 C:\WINDOWS\system32\comctl32.dll.124.Config
   Opens:
                                                 {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\CLR\ Security}
Config\v2.0.50727.42\security.config
                                                 C:\Documents and Settings\Admin\Application Data\Microsoft\CLR Security
   Opens:
Config\v2.0.50727.42\security.config.cch
                                                 C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\index9c.dat
   Opens:
   Opens:
C: \dot{W} INDOWS \ assembly \ Native Images\_v2.0.50727\_32 \ mscorlib \ 9 adb 89 fa 22 fd 5 b 4 ce 43 3 b 5 aca 7 fb 1 b 0 7 \ mscorlib. ni.dll
                                                 C:\WINDOWS\assembly\GAC_32\mscorlib\2.0.0.0_b77a5c561934e089
   Opens:
   Opens:
                                                 C:\WINDOWS\Temp
                                                 C:\WINDOWS\system32\rpcss.dll
   Opens:
                                                 C:\WINDOWS\system32\MSCTF.dll
   Opens:
                                                 C:\WINDOWS\system32\l_intl.nls
   Opens:
                                                 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
   Opens:
   Opens:
                                                 C: \verb|\windows| Microsoft.NET \verb|\windows| first | Solution | Solu
   Opens:
                                                 \label{lem:c:windows} C: \verb|\windows| Microsoft.NET \verb|\Framework| v2.0.50727 \verb|\windows| ms. corjit.dll.2. Configent for the configuration of the configura
   Opens:
                                                 C:\Program Files\Common Files\Microsoft Shared\DW\DW20.EXE
                                                 C:\WINDOWS\system32\apphelp.dll
   Opens:
   Opens:
                                                 {\tt C:\WINDOWS\AppPatch\symmin.sdb}
                                                 C:\WINDOWS\AppPatch\systest.sdb
   Opens:
   Opens:
                                                 C:\Program Files\Common Files\Microsoft Shared\DW
                                                 C:\Program Files
   Opens:
   Opens:
                                                 C:\Program Files\Common Files
                                                 C:\Program Files\Common Files\Microsoft Shared
   Opens:
                                                 C:\PROGRA~1\COMMON~1\MICROS~1\DW\DW20.EXE.Manifest
   Opens:
                                                 C:\PROGRA~1\COMMON~1\MICROS~1\DW\DW20.EXE.Config
   Opens:
                                                 C:\WINDOWS\Prefetch\DW20.EXE-22C39A55.pf
   Opens:
                                                 C:\WINDOWS\system32\oleacc.dll
   Opens:
                                                 C:\WINDOWS\system32\msvcp60.dll
   Opens:
                                                 C:\WINDOWS\system32\oleaccrc.dll
   Opens:
   Opens:
                                                 C:\WINDOWS\system32\SHELL32.dll.124.Manifest
                                                 C:\WINDOWS\system32\SHELL32.dll.124.Config
   Opens:
                                                 {\tt C:\WINDOWS\system32\urlmon.dll.123.Manifest}
   Opens:
   Opens:
                                                 C:\WINDOWS\svstem32\urlmon.dll.123.Config
                                                 C:\WINDOWS\system32\WININET.dll.123.Manifest
   Opens:
                                                 C:\WINDOWS\system32\WININET.dll.123.Config
   Opens:
                                                 C:\WINDOWS\system32\riched20.dll
   Opens:
                                                 C:\WINDOWS\system32\shfolder.dll
   Opens:
   Opens:
                                                 C:\Documents and Settings\Admin\Local Settings\Temp\dw.log
                                                 C:\WINDOWS\system32\psapi.dll
   Opens:
                                                 C:\WINDOWS\system32\ntdl1.dl1
   Opens:
                                                 C:\WINDOWS\system32
   Opens:
                                                 C:\WINDOWS\system32\kernel32.dll
   Opens:
                                                 C:\WINDOWS\system32\advapi32.dll
   Opens:
                                                 C:\WINDOWS\system32\rpcrt4.dll
   Opens:
                                                 C:\WINDOWS\system32\secur32.dll
   Opens:
                                                 C:\WINDOWS\system32\shlwapi.dll
   Opens:
   Opens:
                                                 C:\WINDOWS\system32\gdi32.dll
                                                 C:\WINDOWS\system32\user32.dll
   Opens:
                                                 C:\WINDOWS\system32\msvcrt.dll
   Opens:
                                                 C:\WINDOWS\assembly\NativeImages_v2.0.50727_32
   Opens:
                                                 C:\WINDOWS\system32\ole32.dll
   Opens:
   Opens:
                                                 C:\WINDOWS\system32\version.dll
                                                 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscordacwks.dll
   Opens:
                                                 C:\Documents and Settings\Admin\Local Settings\Temp\A5E762.dmp
   Opens:
                                                 C:\Program Files\Common Files\Microsoft Shared\DW\1033\DWINTL20.DLL
   Opens:
                                                 C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
   Opens:
                                                 C:\Documents and Settings\Admin\Local Settings\Temporary Internet
   Opens:
Files\Content.IE5
   Opens:
                                                 C:\Documents and Settings\Admin\Local Settings\History
                                                C:\Documents and Settings\Admin\Local Settings\History\History.IE5
C:\Documents and Settings\Admin\Local Settings\Temporary Internet
   Opens:
   Opens:
Files\Content.IE5\index.dat
                                                 C:\Documents and Settings\Admin\Cookies
   Opens:
                                                 C:\Documents and Settings\Admin\Cookies\index.dat
   Opens:
                                                 C:\Documents and Settings\Admin\Local
   Opens:
Settings\History\History.IE5\index.dat
                                                 C:\WINDOWS\system32\ws2_32.dll
   Opens:
                                                 C:\WINDOWS\system32\ws2help.dll
   Opens:
   Opens:
                                                 C:\WINDOWS\system32\rasapi32.dll
   Opens:
                                                 C:\WINDOWS\system32\rasman.dll
                                                 C:\WINDOWS\system32\netapi32.dll
   Opens:
                                                 C:\WINDOWS\system32\tapi32.dll
   Opens:
   Opens:
                                                 C:\WINDOWS\system32\rtutils.dll
                                                 C:\WINDOWS\system32\winmm.dll
   Opens:
                                                 C:\WINDOWS\system32\TAPI32.dll.124.Manifest
   Opens:
                                                 C:\WINDOWS\system32\TAPI32.dll.124.Config
   Opens:
                                                 C:\AUTOEXEC.BAT
```

Opens:

Opens: C:\Documents and Settings\All Users\Application

Data\Microsoft\Network\Connections\Pbk

C:\WINDOWS\system32\ras Opens:

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

Data\Microsoft\Network\Connections\Pbk\

Opens: C:\WINDOWS\system32\sensapi.dll Opens: C:\WINDOWS\system32\uxtheme.dll

Opens: C:\WINDOWS\win.ini

Opens: C:\PROGRA~1\COMMON~1\MICROS~1\DW\DW20.EXE.3.Manifest

Opens: C:\WINDOWS\system32\msv1_0.dll Opens: C:\WINDOWS\system32\iphlpapi.dll

Writes to: ${\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\dw.log}$ Writes to: ${\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\A5E762.dmp}$ C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config Reads from:

Reads from: C:\WINDOWS\Temp\6bb534e6c0348b33b54c16dff868e84d.exe

Reads from: C:\AUTOEXEC.BAT Reads from: C:\WINDOWS\win.ini

Windows Registry Events

Creates key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders Creates key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders ${\tt HKLM \ } software \verb|\ microsoft \ \\ fusion \verb|\ gacchangenotification \ \\ \ default$ Creates key:

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

HKLM\software\microsoft\tracing Creates key:

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

settings\connections

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

settings[proxyserver]

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

settings[proxvoverride]

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

settings[autoconfigurl]

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

options\6bb534e6c0348b33b54c16dff868e84d.exe

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

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

options\secur32.dll

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

options\rpcrt4.dll

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

options\advapi32.dll

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

Opens key: HKLM\

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

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

options\ntdll.dll Opens key:

HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll

Opens key: options\mscoree.dll

Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers

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

Opens key: Opens key: HKLM\software\microsoft\.netframework

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

options\user32.dll

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

options\imm32.dll

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

options\gdi32.dll

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\shlwapi.dll

Opens key: HKLM\system\currentcontrolset\control\error message instrument\ Opens key: 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 HKLM\software\microsoft\windows nt\currentversion\ime compatibility Opens key: HKLM\software\microsoft\windows nt\currentversion\windows Opens key:

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

Opens key: Opens key: HKCU\software\microsoft\.netframework\policy\standards HKLM\software\microsoft\.netframework\policy\standards

Opens key: Opens key: HKLM\software\microsoft\.netframework\policy\standards\v2.0.50727

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

Opens key: HKCU\control panel\desktop

Opens key:

 $\label{thm:hklm:software} \begin{tabular}{ll} HKLM \label{thm:software:microsoft:windows:current} \\ \begin{tabular}{ll} HKLM \label{thm:software:microsoft:windows:microsoft:windo$

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

options\msvcr80.dll

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

options\mscorwks.dll

Opens key: HKCU\software\microsoft\.netframework

```
Opens key:
                                                                                                                                                HKLM\software\microsoft\fusion
          Opens key:
                                                                                                                                                HKCU\software\microsoft\fusion
          Opens key:
 \label{thm:local_hammon} \begin{tabular}{ll} HKLM \software \verb|\microsoft|.net framework \security \policy \extensions \named permission sets \end{tabular}
          Opens key:
 HKLM \ software \ microsoft \ .net framework \ security \ policy \ extensions \ named permission sets \ internet
          Opens key:
 HKLM \label{lem:hklm} In the lemma that the lemma
          Opens key:
                                                                                                                                                \label{lem:hklm} \mbox{ HKLM\software\mbox{\sc microsoft\windows nt\currentversion\profilelist\s-1-5-21-profile} \mbox{\sc microsoft\windows nt\currentversion\profilelist\s-1-5-21-profilelist\s-1-5-21-profilelist\s-1-5-21-profilelist\sc microsoft\sc 
  1757981266-507921405-1957994488-1003
         Opens key:
                                                                                                                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\shell32.dll
          Opens key:
                                                                                                                                                  HKLM\system\setup
          Opens key:
                                                                                                                                                \label{local-optimization} \mbox{HKLM} \mbox{$\stackrel{\cdot}{\sc hklm}$ irrosoft\windows nt\currentversion\sc hierarchy} \mbox{$\stackrel{\cdot}{\sc hklm}$ irrosoft\windows nt\currentversion\sc hklm} \mbox{$\stackrel{\cdot}{\sc hklm}$ irrosoft\sc hklm} \mbox{$\stackrel{\cdot}{\sc hklm}
 options\comctl32.dll
          Opens key:
                                                                                                                                                \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ explorer \verb+ \advanced \\
          Opens key:
                                                                                                                                                \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ language pack
                                                                                                                                                Opens key:
          Opens key:
                                                                                                                                                HKLM \verb|\software\microsoft\fusion\native images index \verb|\v2.0.50727_32| \\
          Opens key:
                                                                                                                                                HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus index 9c
          Opens key:
 HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 181938c6 \ 7950e2c5 \ ni \ native images index \ native images \
          Opens key:
 HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 181938c6 \ 7950e2c5 \ 8ex \ new \ ne
          Opens key:
 HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il\ 7950e2c5 \ 3838a3a4 \ 883a3a4 \ and \
          Opens key:
                                                                                                                                                \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
 options\ole32.dll
          Opens key:
                                                                                                                                                HKLM\software\microsoft\ole
          Opens key:
                                                                                                                                                HKCR\interface
                                                                                                                                                HKCR\interface\{00020400-0000-0000-c000-000000000046}
          Opens key:
         Opens key:
                                                                                                                                                \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
  options\mscorlib.ni.dll
          Opens key:
                                                                                                                                                \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution
 options\msctf.dll
          Opens key:
 HKLM\software\microsoft\ctf\compatibility\6bb534e6c0348b33b54c16dff868e84d.exe
          Opens key:
                                                                                                                                                {\it HKLM} \verb|\software\microsoft\ctf\systemshared\| \\
                                                                                                                                                HKCU\keyboard layout\toggle
          Opens key:
                                                                                                                                                HKLM\software\microsoft\ctf\
          Opens kev:
          Opens key:
 \label{tware} \begin{tabular}{ll} HKLM \label{tware} & HKLM \label{tware} \begin{tabular}{ll} HKLM \label{tware} & 1.50727\_32 \label{tware} \begin{tabular}{ll} 1.50727\_32 \label{tware} \begin{tabular
          Opens key:
                                                                                                                                                \label{lem:hklm} \verb+Kklm\+ setup\+ dotnetclient\+ v3.5
          Opens kev:
                                                                                                                                                HKLM\software\microsoft\strongname
          Opens key:
                                                                                                                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
  options\mscorjit.dll
          Opens key:
                                                                                                                                                HKCU\software\policies\microsoft\pchealth\errorreporting
                                                                                                                                                {\tt HKLM} \\ {\tt software \backslash policies \backslash microsoft \backslash pchealth \backslash error reporting}
          Opens kev:
                                                                                                                                                {\tt HKCU \backslash software \backslash microsoft \backslash pchealth \backslash error reporting}
          Opens kev:
          Opens key:
                                                                                                                                                  HKLM\software\microsoft\pchealth\errorreporting
                                                                                                                                                \label{thm:local} \verb+HKCU\+ software\+ policies\+ microsoft\+ pchealth\+ error reporting\+ exclusion list
          Opens key:
                                                                                                                                                \label{thm:local} \verb+HKLM\software\policies\microsoft\pchealth\error reporting\exclusion list
          Opens key:
                                                                                                                                                \label{thm:linear} \mbox{HKCU\software\mbox{\sc microsoft\pchealth\errorreporting\exclusionlist}} \\
          Opens kev:
          Opens key:
                                                                                                                                                HKLM \setminus software \setminus microsoft \setminus pchealth \setminus error reporting \setminus exclusion list
                                                                                                                                                \label{thm:cu} \begin{tabular}{ll} HKCU \software \policies \microsoft \policies \microsoft \policies \microsoft \policies \
          Opens key:
          Opens key:
                                                                                                                                                \label{thm:local} \verb+HKLM\software\policies\microsoft\pchealth\error reporting\nclusion list
                                                                                                                                                \label{thm:local} \verb+HKCU\+ software\+ incresoft\+ pchealth\+ error reporting\+ inclusion list
          Opens key:
          Opens kev:
                                                                                                                                                HKLM\software\microsoft\pchealth\errorreporting\inclusionlist
          Opens key:
                                                                                                                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\version.dll
          Opens key:
                                                                                                                                                HKLM\software\microsoft\pchealth\errorreporting\dw\installed
          Opens key:
                                                                                                                                                HKLM\system\currentcontrolset\control\session manager\appcertdlls
                                                                                                                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
         Opens key:
  options\apphelp.dll
          Opens key:
                                                                                                                                                HKLM\system\wpa\tabletpc
          Opens kev:
                                                                                                                                                HKLM\system\wpa\mediacenter
          Opens kev:
                                                                                                                                                HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
         Opens key:
                                                                                                                                                HKLM\software\microsoft\windows
 \verb|nt\currentversion\appcompatflags\custom\dw20.exe|
                                                                                                                                                HKLM\software\policies\microsoft\windows\safer\levelobjects
          Opens key:
          Opens kev:
                                                                                                                                                HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
          Opens kev:
 be2efd2c1a33}
          Opens kev:
                                                                                                                                                HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
          Opens key:
 edd5fbde1328}
         Opens key:
b813f72dbb91}
          Opens kev:
 7c29ddecae3f}
         Opens key:
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{94e3e076-8f53-42a5-8411-1444, \ name \ na
 085bcc18a68d3
         Opens key:
 HKL\dot{M}\ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0\ hashes \ \{dc971ee5-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4f
 b91490411bfc}
          Opens kev:
\label{lem:hklm} \mbox{HKLM} \mbox{$\tt NSoftware \onicrosoft \onhows \onho
```

Opens key:

```
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ \ 4096 \ paths
   Opens kev:
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ \ 4096 \ has hes
   Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus urlzones
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
   Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus has hes
   Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus urlzones
   Opens key:
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 131072 \ paths
   Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus hashes
   Opens key:
Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus paths
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
   Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus urlzones
   Opens key:
                                          HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus paths
   Opens key:
                                          \label{thm:condition} HKCU \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ \ 0 \ has hes
   Opens key:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \normalle \normal
   Opens key:
HKCU \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ \ 4096 \ paths
   Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus 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
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus urlzones
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
   Opens kev:
                                          HKCU\software\microsoft\windows\currentversion\explorer\shell folders
   Opens kev:
                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dw20.exe
  Opens key:
                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcp60.dll
  Opens kev:
                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleaut32.dll
  Opens key:
                                          \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\oleacc.dll
                                          \label{lem:hklm} \mbox{HKLM\software\mbox{\sc microsoft\windows} nt\current\version\sc file\ execution} \\
  Opens key:
options\iertutil.dll
  Opens key:
                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\urlmon.dll
                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\normaliz.dll
                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens kev:
options\wininet.dll
   Opens key:
                                          HKLM\software\microsoft\oleaut
   Opens key:
                                          HKLM\software\microsoft\oleaut\userera
   Opens kev:
                                          HKCU\software\classes\
   Opens key:
                                          HKCU\software\classes\protocols\name-space handler\
   Opens key:
                                          HKCR\protocols\name-space handler
   Opens key:
                                          HKCU\software\classes\protocols\name-space handler
   Opens key:
                                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings
                                          HKLM\software\microsoft\windows\currentversion\internet settings
  Opens key:
   Opens key:
                                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings
                                          HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_protocol_lockdown
                                          HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature protocol lockdown
  Opens key:
                                          \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \begin{tabular}{ll} policies \end{tabular} internet \end{tabular}
settings\
                                          HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
   Opens kev:
                                          HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
   Opens key:
                                          HKLM\software\microsoft\internet explorer\main\featurecontrol
   Opens kev:
                                          HKCU\software\microsoft\internet explorer\main\featurecontrol
   Opens key:
   Opens kev:
                                          HKCU\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_ignore\_policies\_zonemap\_if\_esc\_enabled\_kb918915
                                         HKLM\software\microsoft\internet
   Opens kev:
```

explorer\main\featurecontrol\feature ignore policies zonemap if esc enabled kb918915

```
Opens key:
                            HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
 Opens key:
                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
 Opens key:
                            HKLM \ software \ policies \ microsoft \ windows \ current version \ internet
settings\zonemap\ranges\
 Opens key:
                            \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\zonemap\ranges\
 Opens key:
                            HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
                            HKLM\software\microsoft\internet
 Opens key:
\verb|explorer\main\featurecontrol\feature\_unc\_savedfilecheck| \\
 Opens key:
                            HKLM\system\currentcontrolset\control\wmi\security
 Opens key:
                            \label{lem:hkcu} \mbox{HKCU\software\mbox{$m$icrosoft\pchealth\errorreporting\dw\debug}} \label{lem:hkcu}
 Opens key:
                           HKLM\software\microsoft\oasys\oaclient
 Opens key:
                            \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\riched20.dll
 Opens key:
                            \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\shfolder.dll
 Opens key:
                            HKLM\software\microsoft\windows\currentversion
 Opens key:
                            HKLM\software\microsoft\office\11.0\common\installroot
 Opens key:
                            HKLM\software\microsoft\ctf\compatibility\dw20.exe
 Opens key:
                            HKCU\software\policies
 Opens key:
                            HKCU\software\policies\microsoft\office\common
 Opens key:
                            HKCU\software
 Opens key:
                            HKCU\software\microsoft\office\common
 Opens key:
                            HKCU\software\microsoft\internet explorer\settings
 Opens key:
                            HKCU\software\microsoft\pchealth\errorreporting\dw
 Opens key:
                            HKLM \setminus software \setminus microsoft \setminus pchealth \setminus error reporting \setminus dw
 Opens key:
                            \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ pchealth\+ error reporting\+ dw\+ debug
 Opens key:
                            \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ pchealth\+ error reporting\+ dw
 Opens key:
                            HKLM\software\policies\microsoft\pchealth\errorreporting\dw
 Opens key:
                            \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\psapi.dll
                            HKLM\software\microsoft\windows nt\currentversion\minidumpauxiliarydlls
 Opens key:
 Opens key:
                            HKLM\software\microsoft\windows
nt\currentversion\knownmanageddebuggingdlls
 Opens key:
                            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mscordacwks.dll
 Opens kev:
                            HKCU\software\microsoft\windows\currentversion\internet settings
 Opens key:
                            HKLM\software\policies
 Opens key:
                            HKLM\software
 Opens key:
                            HKLM\software\policies\microsoft\internet explorer
 Opens kev:
                            HKLM\software\policies\microsoft\internet explorer\main
 Opens key:
                            \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\5.0\cache
                            \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Opens key:
settings\5.0\cache
                            HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0\cache\content
 Opens key:
                            HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
                            HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0\cache\cookies
 Opens key:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
                            HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0\cache\history
 Opens key:
                            HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
                            HKLM\software\microsoft\rpc\pagedbuffers
 Opens key:
                            HKLM\software\microsoft\rpc
 Opens kev:
                            HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens kev:
options\dw20.exe\rpcthreadpoolthrottle
                            HKLM\software\policies\microsoft\windows nt\rpc
 Opens key:
 Opens kev:
                            HKLM\system\currentcontrolset\control\computername
                            HKLM\system\currentcontrolset\control\computername\activecomputername
 Opens kev:
                            HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\extensible cache
 Opens key:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore
                            HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\extensible cache\feedplat
 Opens key:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat
                            HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0cache\ensuremath{\mbox{extensible}} cache\ensuremath{\mbox{ietld}}
                            HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\extensible cache\mshist012014033120140407
                            HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0\cache\extensible cache\mshist012014041220140413
                            HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0\cache\extensible cache\privacie:
                            HKCU\software\microsoft\internet
 Opens key:
\verb|explorer\main\featurecontrol\retry_header on ly post\_on connection reset|\\
                            HKLM\software\microsoft\internet
 Opens kev:
explorer \verb|\main| feature control| retry\_header on ly post\_on connection reset
 Opens key:
                            HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
 Opens kev:
                            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
 Opens key:
                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
```

```
Opens key:
                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
 Opens key:
                    HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
 Opens key:
                   \label{lem:hkcu} \verb+KKCU\+software\+policies\+microsoft\+windows\+currentversion\+internet
settings\5.0\cache
 Opens key:
                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                   HKLM\software\microsoft\internet
 Opens key:
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 key:
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
 Opens key:
                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
 Opens key:
                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
 Opens key:
                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                   HKLM\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature\_allow\_long\_international\_file names| \\
 Opens key:
                   HKCU\software\microsoft\internet
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 key:
                   HKCU\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_disable\_unicode\_handle\_closing\_callback
 Opens key:
                   HKLM\software\microsoft\internet
explorer \verb|\main\feature| on trol\feature\_disable\_unicode\_handle\_closing\_callback
 Opens key:
                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                   HKLM\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature_disallow_null\_in\_response\_headers| \\
 Opens kev:
                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                   HKLM\software\microsoft\internet
explorer \verb|\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:
                   \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\ws2help.dll
 Opens key:
                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
 Opens kev:
                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dwintl20.dll
 Opens key:
                   \label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ services \+ winsock 2 \+ parameters
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
 Opens kev:
Opens key:
Opens key:
Opens key:
Opens kev:
Opens kev:
Opens key:
Opens kev:
Opens key:
Opens kev:
HKLM \ system \ \ current control set \ services \ \ winsock 2 \ parameters \ protocol\_catalog 9 \ \ catalog\_entries \ \ 000000000010
 Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
 Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
 Opens kev:
Opens kev:
Opens kev:
HKLM\svstem\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\0000000000003
```

Opens key: $\begin{tabular}{ll} HKCU\software\microsoft\windows\currentversion\internet settings\wpad \\ HKCU\software\microsoft\internet \\ \end{tabular}$

```
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens kev:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netapi32.dll
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasman.dll
  Opens key:
                                    \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\rtutils.dll
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winmm.dll
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\drivers32
  Opens key:
Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\tapi32.dll
  Opens key:
                                     HKLM\software\microsoft\windows\currentversion\telephony
                                    \label{lem:hklm} \mbox{HKLM\software\mbox{\sc microsoft\windows} nt\current\version\sc mage} \ \ \mbox{file execution}
  Opens key:
options\rasapi32.dll
  Opens key:
                                    HKLM\software\microsoft\tracing\rasapi32
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\userenv.dll
  Opens key:
                                    Opens key:
                                    HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Opens key:
                                    HKLM\software\policies\microsoft\windows\system
  Opens key:
                                    \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows nt + current version + profile list
  Opens key:
                                     HKLM\system\currentcontrolset\control\session manager\environment
  Opens key:
                                    HKU\
  Opens key:
                                    HKCU\environment
  Opens key:
                                    HKCU\volatile environment
  Opens key:
                                    \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\sensapi.dll
  Opens key:
                                    \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution
options\uxtheme.dll
  Opens key:
                                    HKCU\software\microsoft\windows\currentversion\thememanager
  Opens key:
                                    HKCU\software\microsoft\windows nt\currentversion\windows
  Opens key:
                                    HKLM\system\currentcontrolset\control\nls\locale
  Opens key:
                                    HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
  Opens kev:
                                    \label{lem:hklm} \verb+ HKLM \ system \ current control \ \ language groups
  Opens key:
                                    HKLM\software\microsoft\rpc\securityservice
  Opens key:
                                     HKLM\system\currentcontrolset\control\securityproviders
  Opens key:
                                    {\tt HKLM \ } system \verb|\ current control \ \\ lsa \ \\ sspicache \verb|\ msapsspc.dll|
  Opens key:
  Opens key:
                                    \label{lem:hklm} \verb+Kklm \system \current control \spic ache \spi
  Opens key:
                                    HKLM \ system \ current control \ lsa \ sspicache \ msnsspc. dll
  Opens key:
                                    HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\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
                                    \label{lem:hklm} \mbox{HKLM} \mbox{`software} \mbox{`microsoft} \mbox{`windows nt} \mbox{`currentversion} \mbox{`image file execution}
  Opens kev:
options\msv1_0.dll
  Oueries value:
HKLM \verb|\software| policies \verb|\microsoft| windows \verb|\safer| code identifiers [transparentenabled]|
  Oueries value:
                                    HKLM\svstem\currentcontrolset\control\terminal server[tsappcompat]
                                    {\tt HKLM \ } system \verb| current control \verb| session manager[safedll search mode] \\
  Queries value:
  Queries value:
                                    \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ winlogon [leaktrack]
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
  Oueries value:
options\mscoree.dll[checkapphelp]
  Oueries value:
                                    HKLM\system\currentcontrolset\control\session
manager\appcompatibility[disableappcompat]
                                    HKLM\software\microsoft\.netframework[installroot]
  Oueries value:
  Oueries value:
                                    HKLM\software\microsoft\.netframework[clrloadlogdir]
                                    HKLM\software\microsoft\.netframework[onlyuselatestclr]
  Oueries value:
  Oueries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Oueries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\compatibility32[6bb534e6c0348b33b54c16dff868e84d]
                                    HKLM\software\microsoft\windows nt\currentversion\ime
  Oueries value:
compatibility[6bb534e6c0348b33b54c16dff868e84d]
                                    \label{lem:hklm} \mbox{HKLM\software\mbox{$\mbox{$m$icrosoft\windows}$ nt\currentversion\windows[appinit\_dlls]} \\
  Oueries value:
  Oueries value:
                                    HKCU\control panel\desktop[multiuilanguageid]
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
  Oueries value:
options\mscorwks.dll[checkapphelp]
  Oueries value:
                                     HKLM\software\microsoft\.netframework[gcstressstart]
  Oueries value:
                                    HKLM\software\microsoft\.netframework[gcstressstartatjit]
                                    {\tt HKLM \setminus software \setminus microsoft \setminus .net framework [disable config cache]}
  Oueries value:
                                    HKLM\software\microsoft\fusion[cachelocation]
  Oueries value:
  Oueries value:
                                    HKLM\software\microsoft\fusion[downloadcachequotainkb]
  Oueries value:
                                    HKLM\software\microsoft\fusion[enablelog]
                                     HKLM\software\microsoft\fusion[logginglevel]
  Oueries value:
  Oueries value:
                                    HKLM\software\microsoft\fusion[forcelog]
                                    HKLM\software\microsoft\fusion[logfailures]
  Oueries value:
  Oueries value:
                                    HKLM\software\microsoft\fusion[versioninglog]
                                     HKLM\software\microsoft\fusion[logresourcebinds]
  Oueries value:
                                    HKLM\software\microsoft\fusion[uselegacyidentityformat]
  Queries value:
                                    HKLM\software\microsoft\fusion[disablemsipeek]
  Oueries value:
  Oueries value:
                                    HKLM\software\microsoft\fusion[noclientchecks]
  Oueries value:
                                    HKLM\system\setup[systemsetupinprogress]
```

HKCU\control panel\desktop[smoothscroll]

Queries value:

Oueries value: $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus advanced [enable balloon tips]$ Queries value: $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ user shell$ folders[appdata] Queries value: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 [latest index]$ Queries value: $\label{lem:hklm} \begin{tabular}{ll} HKLM \software \microsoft \fusion \native images in dex \norm{v2.0.50727_32$ \ index \norm{gc[nius agemask]}$} \end{tabular}$ Queries value $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 \setminus index 9c[il usage mask]$ Oueries value: $HKLM \ software \ `microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni\ 181938c6 \ 7950e2c5 \ [displayname]$ Queries value $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 181938c6 \ 7950e2c5 \ 8[configmask]$ Oueries value: $HKLM \ software \ `microsoft \ fusion \ native images index \ v2.0.50727_32 \ inl 181938c6 \ 7950e2c5 \ 8 \ [configstring]$ Queries value $HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727_32 \ in \ 181938c6 \ 7950e2c5 \ 8 \ [mvid]$ Oueries value: $HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727_32 \ ni \ 181938c6 \ 7950e2c5 \ [evalation data]$ Oueries value: Queries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 181938c6 \ 7950e2c5 \ 8[ildependencies]$ Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[nidependencies] Queries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 181938c6 \ 7950e2c5 \ 8 \ [missing dependencies]$ Queries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 7950e2c5 \ 3838a3a4 \ 8[displayname]$ Queries value: $HKLM \verb|\software| microsoft \verb|\fusion| native images index \verb|\v2.0.50727_32 \verb|\il| 1 | 7950e2c5 \verb|\software| saa4 \verb|\s$ Queries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 7950e2c5 \ 3838a3a4 \ [modules]$ Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il \ 7950e2c5 \ 3838a3a4 \ 8[sig] \ for the software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il \ native \ mages \ native \ nati$ Queries value: $HKLM \ software \ `microsoft \ fusion \ `native images index \ `v2.0.50727_32 \ il\ \ 7950e2c5 \ \ 3838a3a4 \ \ \ [last mod time]$ Oueries value: HKLM\software\microsoft\fusion\gacchangenotification\default[mscorlib,2.0.0.0,,b77a5c561934e089,x86] Oueries value: HKLM\system\currentcontrolset\control\session manager[criticalsectiontimeout] Oueries value: ${\tt HKLM \setminus software \setminus microsoft \setminus ole[rwlock resource timeout]}$ Oueries value: HKCR\interface[interfacehelperdisableall] Queries value: HKCR\interface[interfacehelperdisableallforole32] Queries value: HKCR\interface[interfacehelperdisabletypelib] Oueries value: HKCR\interface\{00020400-0000-0000-c000-00000000046}[interfacehelperdisableall] HKCR\interface\{00020400-0000-0000-c000-Oueries value: 00000000046}[interfacehelperdisableallforole32] Queries value: ${\tt HKLM \setminus software \setminus microsoft \setminus ctf \setminus systems hared [cuas]}$ Oueries value: HKCU\keyboard layout\toggle[language hotkey] Oueries value: HKCU\keyboard layout\toggle[hotkey] Oueries value: HKCU\keyboard layout\toggle[layout hotkey] Queries value: HKLM\software\microsoft\ctf[enableanchorcontext] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[cache] Oueries value: HKLM\software\microsoft\pchealth\errorreporting[forcequeuemode] Queries value: HKLM\software\microsoft\pchealth\errorreporting[showui] Queries value: HKLM\software\microsoft\pchealth\errorreporting[doreport] Oueries value: HKLM\software\microsoft\pchealth\errorreporting[allornone] Oueries value: $HKLM\software\microsoft\pchealth\errorreporting\exclusionlist[6bb534e6c0348b33b54c16dff868e84d.exe]$ Oueries value: $HKLM \label{lem:hklm} In the latest and the lates$ Oueries value: HKLM\software\microsoft\pchealth\errorreporting\dw\installed[dw0200] Oueries value: HKLM\svstem\wpa\mediacenter[installed] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834dbe2efd2c1a33}[itemdata] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834dbe2efd2c1a33}[saferflags] Oueries value: edd5fbde1328}[itemdata] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89edd5fbde1328}[hashalg] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89edd5fbde1328}[itemsize] Oueries value: edd5fbde1328}[saferflags] Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57bb813f72dbb91}[itemdata] Oueries value:

```
b813f72dbb91}[hashalg]
     Oueries value:
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{7fb9cd2e-3076-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57
b813f72dbb91}[itemsize]
     Queries value:
b813f72dbb91}[saferflags]
     Queries value:
7c29ddecae3f}[itemdata]
     Oueries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes \setminus \{81d1fe15-dd9d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16
7c29ddecae3f}[hashalg]
     Oueries value:
7c29ddecae3f}[itemsize]
     Queries value:
7c29ddecae3f}[saferflags]
     Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemdata]
     Oueries value:
085bcc18a68d}[hashalg]
     Oueries value:
085bcc18a68d}[itemsize]
     Oueries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes \setminus \{94e3e076-8f53-42a5-8411-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-14414-1441-144
085bcc18a68d}[saferflags]
     Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemdata]
     Oueries value:
b91490411bfc}[hashalg]
     Oueries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes \setminus \{dc971ee5-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe
b91490411bfc}[itemsize]
     Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[saferflags]
     Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
     Queries value:
HKLM \verb|\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]|
     Oueries value:
                                                                     HKCU\software\microsoft\windows\currentversion\explorer\shell
 folders[cache]
     Queries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [log filename]
     Oueries value:
                                                                     HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
     Oueries value:
                                                                     HKLM\software\microsoft\windows nt\currentversion\compatibility32[dw20]
     Oueries value:
                                                                     HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[dw20]
                                                                     HKLM\software\microsoft\windows\currentversion\internet
     Queries value:
 settings[disableimprovedzonecheck]
     Oueries value:
                                                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[dw20.exe]
     Queries value:
                                                                     HKLM\software\microsoft\internet
 explorer\main\featurecontrol\feature protocol lockdown[*]
     Oueries value:
                                                                     HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
 ab78-1084642581fb1
     Oueries value:
                                                                     HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
 0000-00000000000001
     Oueries value:
                                                                     HKLM\software\microsoft\windows\currentversion[programfilesdir]
     Oueries value:
                                                                     HKLM\software\microsoft\windows\currentversion[commonfilesdir]
                                                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
     Oueries value:
 folders[personal]
     Queries value:
                                                                     HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
                                                                     HKCU\software\microsoft\office\common[amstrmax]
     Oueries value:
                                                                     HKCU\software\microsoft\office\common[qmstudyid]
     Queries value:
     Oueries value:
                                                                     HKCU\software\microsoft\internet explorer\settings[anchor color]
     Oueries value:
HKLM \verb|\software\microsoft\pchealth\error reporting \verb|\dw[dwclosetransferdialogwhendone]| \\
                                                                     HKLM\software\microsoft\pchealth\errorreporting\dw[dwfiletreeroot]
     Oueries value:
     Oueries value:
                                                                     HKLM\software\microsoft\pchealth\errorreporting\dw[dwtracking]
                                                                     HKLM\software\microsoft\pchealth\errorreporting\dw[dwnoexternalurl]
     Oueries value:
                                                                     HKLM\software\microsoft\pchealth\errorreporting\dw[dwnofilecollection]
     Oueries value:
     Oueries value:
HKLM \setminus software \setminus microsoft \setminus pchealth \setminus error reporting \setminus dw[dwnosecondlevel collection]
     Oueries value:
                                                                     HKLM\software\microsoft\pchealth\errorreporting\dw[dwurllaunch]
                                                                     HKLM\software\microsoft\pchealth\errorreporting\dw[dwneverupload]
     Oueries value:
                                                                     HKLM\software\microsoft\pchealth\errorreporting\dw[dwreporteename]
     Oueries value:
```

HKLM\software\microsoft\pchealth\errorreporting\dw[dwqueuepesterinterval]

Queries value: HKLM\software\microsoft\pchealth\errorreporting\dw[dwverboselog]

Queries value: Oueries value:

Oueries value:

Queries value: HKLM\software\microsoft\pchealth\errorreporting\dw[dwerbosetog]
Queries value: HKLM\software\microsoft\pchealth\errorreporting\dw[dwalwaysreport]

HKLM\software\microsoft\pchealth\errorreporting\dw[dwnocollectionlink]

HKLM\software\microsoft\pchealth\errorreporting\dw[dwmaxqueuesize]

HKLM\software\microsoft\pchealth\errorreporting\dw[dwnosignoffqueuereporting]

```
Oueries value:
                                                                                           HKLM\software\microsoft\pchealth\errorreporting\dw[dwexplainerurl]
     Oueries value:
                                                                                           HKLM\software\microsoft\pchealth\errorreporting\dw[dwbypassqueue]
      Queries value:
                                                                                           HKLM \setminus software \setminus microsoft \setminus pchealth \setminus error reporting \setminus dw[dwall queue sheadless]
                                                                                           HKLM\software\microsoft\windows
     Queries value:
nt\currentversion\minidumpauxiliarydlls[c:\windows\temp\6bb534e6c0348b33b54c16dff868e84d.exe]
                                                                                           HKLM\software\microsoft\windows
     Oueries value:
nt\currentversion\minidumpauxiliarydlls[c:\windows\system32\ntdll.dll]
                                                                                           HKLM\software\microsoft\windows
     Queries value:
nt\currentversion\minidumpauxiliarydlls[c:\windows\system32\mscoree.dll]
                                                                                           HKLM\software\microsoft\windows
     Queries value:
nt\currentversion\minidumpauxiliarydlls[c:\windows\system32\kernel32.dll]
     Queries value:
                                                                                           HKLM\software\microsoft\windows
nt \verb|\current version \verb|\minidum pauxiliary dlls[c:\windows \verb|\system32 advapi32.dll]| \\
                                                                                           HKLM\software\microsoft\windows
     Queries value:
nt\currentversion\minidumpauxiliarydlls[c:\windows\system32\rpcrt4.dll]
                                                                                           HKLM\software\microsoft\windows
     Queries value:
nt\currentversion\minidumpauxiliarydlls[c:\windows\system32\secur32.dll]
                                                                                           HKLM\software\microsoft\windows
     Queries value:
nt\currentversion\minidumpauxiliarydlls[c:\windows\system32\shlwapi.dll]
                                                                                           HKLM\software\microsoft\windows
     Queries value:
nt\current version\mbox{\colored} in tarydlls \cite{c:windows\system32\gdi32.dll} \cite{c:windows\sy
                                                                                           HKLM\software\microsoft\windows
     Queries value:
nt\currentversion\minidumpauxiliarydlls[c:\windows\system32\user32.dll]
                                                                                           HKLM\software\microsoft\windows
     Queries value:
\verb| nt\current version\minidum pauxiliary dlls[c:\windows\system32\msvcrt.dll]| \\
     Queries value:
                                                                                           HKLM\software\microsoft\windows
nt\currentversion\minidumpauxiliarydlls[c:\windows\system32\imm32.dll]
     Queries value:
                                                                                           HKLM\software\microsoft\windows
\verb| nt\currentversion\minidum pauxiliary dlls[c:\windows\microsoft.net\framework\v2.0.50727\mscorwks.dll]| | the continuous of the contin
                                                                                           HKLM\software\microsoft\windows
     Queries value:
nt\corrent version\mbox{\corrent} iarydlls[c:\mbox{\corrent} iarydlls[c:\mbox{\corrent} iarydlls]] and the corrent version\mbox{\corrent} iarydlls]] and the correct version\corrent version\mbox{\corrent} iarydlls]] and the correct version\mbox
ww b80fa8ca\msvcr80.dll1
     Queries value:
                                                                                           HKLM\software\microsoft\windows
nt \verb|\currentversion\minidumpauxiliarydlls[c:\windows\system32\shell32.dll]|
     Oueries value:
                                                                                           HKLM\software\microsoft\windows
\verb| nt\currentversion\minidumpauxiliarydlls[c:\windows\winsxs\x86_microsoft.windows.common-relation and the common-relation of the common com
controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll]
                                                                                           HKLM\software\microsoft\windows
     Queries value:
nt\current version\mbox{\comctl32.dll}]
     Oueries value:
                                                                                           HKLM\software\microsoft\windows
nt\current version\mbox{\colored} has been all of the continuous and the continuous has been by notive images $$v2.0.50727_32\mbox{\colored} has been all of the continuous has been all
     Queries value:
                                                                                           HKLM\software\microsoft\windows
nt\current version\mbox{\colored} in tarydlls \cite{c:windows\system32\ole32.dll} \cite{c:windows\sy
     Oueries value:
                                                                                           HKLM\software\microsoft\windows
nt\currentversion\minidumpauxiliarydlls[c:\windows\system32\msctf.dll]
     Queries value:
                                                                                           HKLM\software\microsoft\windows
nt \verb|\colored| to the continuous of the contin
     Oueries value:
                                                                                           HKLM\software\microsoft\windows
nt \verb|\currentversion\minidumpauxiliarydlls[c:\windows\system32\version.dll]|
     Queries value:
                                                                                           HKLM\software\microsoft\windows
nt\currentversion\minidumpauxiliarydlls[c:\windows\system32\apphelp.dll]
     Queries value:
                                                                                           HKLM\software\microsoft\windows
nt\currentversion\knownmanageddebuggingdlls[c:\windows\microsoft.net\framework\v2.0.50727\mscordacwks.dll]
     Oueries value:
                                                                                           HKCU\software\microsoft\windows\currentversion\internet
{\tt settings[fromcachetimeout]}
     Queries value:
                                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
     Oueries value:
                                                                                           HKLM\software\policies\microsoft\internet
explorer\main[security_hklm_only]
     Queries value:
                                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
     Oueries value
                                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
     Queries value:
                                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
     Oueries value:
                                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
                                                                                           HKCU\software\microsoft\windows\currentversion\internet
     Queries value:
settings[cachemode]
     Queries value:
                                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
                                                                                           HKCU\software\microsoft\windows\currentversion\internet
     Queries value:
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:
                                                                                           HKCU\software\microsoft\internet
explorer\main\featurecontrol[feature clientauthcertfilter]
     Oueries value:
                                                                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
     Oueries value:
                                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
     Oueries value:
                                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
     Oueries value:
                                                                                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
     Oueries value:
                                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[signature]
                                                                                           HKCU\software\microsoft\windows\currentversion\internet
     Oueries value:
settings\5.0\cache\content[peruseritem]
                                                                                           HKLM\software\microsoft\windows\currentversion\internet
     Oueries value:
```

settings\5.0\cache\content[peruseritem]

```
HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\content[cacheprefix]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cachelimit]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\cookies[peruseritem]
  Queries value:
                                  HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
                                  \label{lem:hkcu} \verb+KKCU\+software\+microsoft\+windows\+currentversion\+explorer\+user\ shell
  Queries value:
folders[cookies]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\cookies[cacheprefix]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\cookies[cachelimit]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\history[peruseritem]
  Queries value:
                                   HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
\verb|settings\5.0\cache\history[cacheprefix]|\\
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
  Queries value:
                                   HKLM\software\microsoft\rpc[maxrpcsize]
  Oueries value:
Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacherepair]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachepath]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheprefix]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
  Queries value:
                                  \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings\5.0\cache\extensible cache\domstore[cacheoptions]
  Queries value:
                                  \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\5.0\cache\extensible cache\feedplat[cacherepair]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings \verb|\5.0| cache \verb|\extensible| cache \verb|\feedplat[cacheprefix]|
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
  Oueries value:
                                  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]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
  Oueries 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]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
  Oueries value
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
  Oueries value
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings \verb|\| 5.0 \verb|\| cache \verb|\| extensible | cache \verb|\| mshist012014033120140407 [cacherepair] | cacherepair |
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\privacie:[cacherepair]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\privacie:[cachepath]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
```

settings\5.0\cache\extensible cache\privacie:[cacheprefix]

```
settings\5.0\cache\extensible cache\privacie:[cachelimit]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
 Queries 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]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketreceivebufferlength]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[keepalivetimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings[maxconnectionsperserver]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings[maxconnectionsper1_0server]
 Queries value:
                           \label{lem:hklm} \verb+ HKLM \+ software \+ microsoft \+ windows \+ current version \+ internet
settings[maxconnectionsper1_0server]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings[maxconnectionsperproxy]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[serverinfotimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[connectretries]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings[disablentlmpreauth]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
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]
 Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
 Oueries value:
                           HKLM\software\microsoft\internet
explorer \verb|\main\feature| closing_callback[dw20.exe]|
 Oueries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[leashlegacycookies]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablent4rascheck]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dialupuselansettings]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dialupuselansettings]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypassftptimecheck]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[releasesocketduringauth]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
                           \label{lem:hklm} \verb+Kklm\+ software\+ icrosoft\+ windows\+ current version\+ internet
 Oueries value:
settings[releasesocketduring401auth]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[wpadsearchalldomains]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablelegacypreauthasserver]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
```

HKCU\software\microsoft\windows\currentversion\internet

Oueries value:

```
settings[disablelegacypreauthasserver]
                     HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasshttpnocachecheck]
                     \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} internet \end{tabular}
 Queries value:
{\tt settings[bypasshttpnocachecheck]}
                     HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasssslnocachecheck]
                     HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasssslnocachecheck]
                     HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[enablehttptrace]
 Queries value:
                     HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
                     \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings[nocheckautodialoverride]
 Queries value:
                     HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                     \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings[dontusednsloadbalancing]
 Queries value:
                     HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
 Queries value:
                     \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings[mimeexclusionlistforcache]
 Queries value:
                     HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
 Queries value:
                     HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
 Queries value:
                     HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
 Queries value:
                     \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[dnscachetimeout]
 Queries value:
                     HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
 Queries value:
                     HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
 Queries value:
                     HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
 Queries value:
                     \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[warnonbadcertsending]
 Oueries value:
                     HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
 Queries value:
                     HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
 Queries value:
                     HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
 Queries value:
                     HKCU\software\microsoft\windows\currentversion\internet
{\tt settings[warnonhttpstohttpredirect]}
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
 Oueries value:
HKLM \land system \land current control set \land services \land winsock 2 \land parameters \land protocol\_catalog 9 [num\_catalog\_entries]
 Queries value:
Oueries value
Queries value:
Oueries value
Queries value:
Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000006[packedcatalogitem]
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000008[packedcatalogitem]
 Oueries value:
Oueries value:
Oueries value:
Oueries value:
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 \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ set \ log\_entries \ 000000000001 \ [library path]
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[supportednamespace]
 Oueries value:
```

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001[enabled]

Oueries value: Queries value: $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog5 \ catalog_entries \ 00000000001[stores service class info]]$ Queries value: Queries value: $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries \ 000000000002 \ [displaystring]$ Queries value: $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 0000000000002 [providerid]$ Queries value: Queries value: Oueries value: Queries value: $HKLM \ system \ \ current control set \ services \ \ winsock 2 \ parameters \ \ namespace_catalog 5 \ \ \ catalog_entries \ \ \ 000000000002 \ \ \ [version]$ Queries value: $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog5 \ catalog_entries \ 00000000000002 [storesserviceclass info]]$ Oueries value: $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ (catalog_entries) \ 0000000000003 \ [library path]$ Queries value: $HKLM \ system \ current controls et \ services \ \ win sock 2 \ parameters \ names pace_catalog5 \ catalog_entries \ \ \ 000000000003 \ [displaystring]$ Queries value: Queries value: $HKLM \ system \ current controls et \ services \ \ winsock 2 \ parameters \ names pace_catalog5 \ catalog_entries \ \ \ 000000000003 \ [address family]$ Queries value: Queries value: Queries value: Oueries value: $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog5 \ catalog_entries \ 00000000003 \ [storesserviceclassinfo]$ Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets] Oueries value: HKLM\svstem\currentcontrolset\services\winsock2\parameters[ws2 32spincount1 Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[globaluseroffline] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[enableautodial] Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[urlencoding] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[truncatefilename] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[badproxyexpirestime] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midil] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7] Oueries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9] Oueries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1] Queries 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] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8] Oueries value:

Oueries value: HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel] HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1] Oueries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2] HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer31 Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9] Oueries value: Queries value:

HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]

Oueries value:

```
Oueries value:
HKLM \label{lem:hklm} In the latest and the lates
   Queries value:
                                             HKLM\software\microsoft\tracing[enableconsoletracing]
   Oueries value:
                                             HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
   Oueries value:
                                             HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
   Oueries value:
                                             HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
   Queries value:
                                             HKLM \setminus software \setminus microsoft \setminus tracing \setminus rasapi32[consoletracing mask]
   Queries value:
                                             HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
   Oueries value:
                                             HKLM\software\microsoft\tracing\rasapi32[filedirectory]
   Queries value:
                                             HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common appdata]
   Queries value:
                                             HKLM\software\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
   Queries value:
                                             HKLM\software\microsoft\windows
nt\currentversion\winlogon[chkaccdebuglevel]
   Queries value:
                                             {\tt HKLM \ } system \verb| current control \verb| set \verb| control \verb| product options[product type]|
   Oueries value:
                                             \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ user shell
folders[local settings]
   Queries value:
                                             HKLM\software\microsoft\windows
nt\currentversion\winlogon[rsopdebuglevel]
   Queries value:
                                             HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
   Oueries value:
                                             HKLM\software\microsoft\windows
nt\currentversion\profilelist[profilesdirectory]
  Oueries value:
                                             HKLM\software\microsoft\windows
nt\currentversion\profilelist[allusersprofile]
   Oueries value:
                                             HKLM\software\microsoft\windows
nt\currentversion\profilelist[defaultuserprofile]
  Oueries value:
                                             HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[profileimagepath]
  Queries value:
                                             HKCU\software\microsoft\windows
nt\currentversion\winlogon[parseautoexec]
  Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
  Oueries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
  Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
  Oueries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
                                              HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[autoconfigurl]
                                             \label{local-observation} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt local-observation} \mbox{\tt internet} \mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt local-observation} \mbox{\tt local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-observation\color=local-obser
  Oueries value:
settings\connections[savedlegacysettings]
   Oueries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
                                             \label{thm:linear} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ irrentversion \thememanager[compositing]} \end{tabular}
   Oueries value:
   Oueries value:
                                             HKCU\control panel\desktop[lamebuttontext]
                                             HKCU\software\microsoft\windows nt\currentversion\windows[scrollinset]
   Oueries value:
   Queries value:
                                             HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
   Oueries value:
                                             HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]
   Oueries value:
                                             HKCU\software\microsoft\windows nt\currentversion\windows[scrolldelay]
   Oueries value:
                                             HKCU\software\microsoft\windows
nt\currentversion\windows[scrollinterval]
                                             Queries value:
   Oueries value:
                                             HKLM\system\currentcontrolset\control\nls\language groups[1]
   Oueries value:
                                             HKLM\software\microsoft\rpc\securityservice[10]
   Oueries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
                                             HKLM \verb|\system| current controlset \verb|\control| lsa \verb|\sspicache| msapsspc.dll[name]|
   Oueries value:
   Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]
   Oueries value:
Oueries value:
                                             HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]
   Oueries value:
HKLM\svstem\currentcontrolset\control\lsa\sspicache\msapsspc.dll[version]
                                             HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]
   Oueries value:
   Oueries value:
\label{local_ham} \begin{tabular}{ll} HKLM\system\currentcontrolset\control\lsa\sspicache\mbox{\system}. dll[tokensize] \\ \end{tabular}
                                             HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]
   Oueries value:
                                             HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]
   Oueries value:
   Oueries value:
HKLM \setminus system \setminus current control \\ lsa \setminus sspicache \setminus digest. \\ dll[capabilities]
   Oueries value:
                                             HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version]
   Oueries value:
                                             HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]
   Oueries value:
   Oueries value:
HKLM \setminus system \setminus current control \setminus lsa \setminus sspicache \setminus digest. dll[tokensize]
                                             HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name]
   Oueries value:
                                             HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment]
   Oueries value:
   Oueries value:
HKLM \setminus system \setminus current control \setminus lsa \setminus sspicache \setminus msnsspc.dll[capabilities]
                                             HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid]
   Oueries value:
                                             HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version]
   Oueries value:
                                             HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type]
   Oueries value:
   Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize]
                                             HKCU\software\microsoft\windows\currentversion\explorer\shell
   Value changes:
folders[appdata]
                                             HKLM\software\microsoft\cryptography\rng[seed]
   Value changes:
   Value changes:
                                             HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
```

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

folders[personal]

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

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} windows \end{tabular} current version \end{tabular} explorer \end{tabular} software \end{tabular} windows \end{tabular} current version \end{tabular} explorer \end{tabular} software \end{tabular} windows \end{tabular} consider \end{tabular} windows \e$

 $\begin{tabular}{ll} folders[cookies] & & & \\ Value changes: & HKCU\software\microsoft\windows\currentversion\explorer\shell \\ folders[history] & & \\ \end{tabular}$

Value changes: folders[common appdata]

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

settings[proxyenable]

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

 ${\tt settings \backslash connections [savedlegacy settings]}$