# Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3316, Task ID: 772

Task ID: 772 Risk Level:

Date Processed: 2016-05-18 10:36:27 (UTC)

Processing Time: 61.57 seconds Virtual Environment: IntelliVM

**Execution Arguments:** "c:\windows\temp\5700c49f29b6358692ee50cb31d7ad54.exe"

Sample ID: Type: basic admin Owner:

5700c49f29b6358692ee50cb31d7ad54 Label:

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

PE32:win32:gui File Type: File Size: 1134080 bytes

5700c49f29b6358692ee50cb31d7ad54 MD5:

176367233358560fca93c53a1ffd73d4d91b1c2daba2f1eaacd2d0c2f509098c SHA256:

Description: None

## Pattern Matching Results

Writes to memory of system processes

- Modifies registry autorun entries
- 3 Program causes a crash [Info]
- Imports registry (\*.REG) file
- Dumps and runs batch script
- 6 Starts process from Application Data folder
- 4 Reads process memory
- Sends FTP commands over the control channel
- 6 Creates executable in application data folder
- 5 Modifies Windows Registry from the command line
- 2 PE: Nonstandard section
- 7 Attempts to connect to dynamic DNS
- 4 Terminates process under Windows subfolder
- 5 Creates process in suspicious location
- Connects to IRC server
- 5 Adds autostart object
- 7 Injects thread into Windows process

#### Static Events

Anomaly: PE: Contains one or more non-standard sections

### Process/Thread Events

C:\WINDOWS\Temp\5700c49f29b6358692ee50cb31d7ad54.exe Creates process:

["c:\windows\temp\5700c49f29b6358692ee50cb31d7ad54.exe" ] C:\WINDOWS\system32\cmd.exe [cmd /c Creates process:

""C:\DOCUME~1\Admin\LOCALS~1\Temp\cpeGx.bat" "]

C:\WINDOWS\system32\reg.exe [REG ADD Creates process:

"HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "Run32.dll" /t REG\_SZ /d "C:\Documents

and Settings\Admin\Application Data\Run32.exe" /f]

C:\Documents and Settings\Admin\Application Data\Run32.exe Creates process:

["C:\Documents and Settings\Admin\Application Data\Run32.exe"]

C:\Documents and Settings\Admin\Application Data\Run32.exe ["C:\Documents and Settings\Admin\Application Data\Run32.exe"]

Creates process: C:\WINDOWS\system32\dwwin.exe [C:\WINDOWS\system32\dwwin.exe -x -s 1464]

RASMAN [C:\WINDOWS\system32\svchost.exe -k netsvcs] Loads service: PID:1048 C:\WINDOWS\system32\calc.exe Reads from process:

Reads from process: PID:1992 C:\WINDOWS\explorer.exe

PID:336 C:\Documents and Settings\Admin\Application Data\Run32.exe Writes to process:

PID:1992 C:\WINDOWS\explorer.exe Writes to process: Terminates process: C:\WINDOWS\system32\reg.exe Terminates process: C:\WINDOWS\system32\cmd.exe

C:\WINDOWS\Temp\5700c49f29b6358692ee50cb31d7ad54.exe Terminates process: Terminates process: C:\Documents and Settings\Admin\Application Data\Run32.exe

Creates remote thread: C:\WINDOWS\explorer.exe

## Named Object Events

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

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

1957994488-1003

```
\BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-
 Creates mutex:
507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003
                          \BaseNamedObjects\ZonesCounterMutex
 Creates mutex:
 Creates mutex:
                          \BaseNamedObjects\ZoneAttributeCacheCounterMutex
 Creates mutex:
                          \BaseNamedObjects\ZonesCacheCounterMutex
 Creates mutex:
                          \verb|\BaseNamedObjects\ZonesLockedCacheCounterMutex| \\
 Creates mutex:
                          \BaseNamedObjects\SHIMLIB_LOG_MUTEX
                          \BaseNamedObjects\SKCJERmeGREBR
 Creates mutex:
                          \BaseNamedObjects\MSCTF.Shared.MUTEX.ANH
 Creates mutex:
 Creates mutex:
                          \BaseNamedObjects\c:!documents and settings!admin!local
```

settings!temporary internet files!content.ie5!

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

settings!history!history.ie5!

\BaseNamedObjects\WininetConnectionMutex Creates mutex:

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

\BaseNamedObjects\CTF.ThreadMarshalInterfaceEvent.000000E0.00000000.00000004

Creates event: \BaseNamedObjects\CTF.ThreadMIConnectionEvent.000000E0.00000000.00000004

\BaseNamedObjects\MSCTF.SendReceive.Event.AO.IC Creates event:

\BaseNamedObjects\MSCTF.SendReceiveConection.Event.AO.IC Creates event:

Creates event: \BaseNamedObjects\MSCTF.SendReceive.Event.ANH.IC

Creates event: \BaseNamedObjects\MSCTF.SendReceiveConection.Event.ANH.IC

\BaseNamedObjects\C:?WINDOWS?TEMP?5700C49F29B6358692EE50CB31D7AD54.EXE Creates semaphore: Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1} \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57} Creates semaphore: Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D} Creates semaphore: \BaseNamedObjects\C:?DOCUMENTS AND SETTINGS?ADMIN?APPLICATION DATA?

RUN32.FXF

Opens:

Creates semaphore: \BaseNamedObjects\MsoDWExclusive1992

C:\WINDOWS

File System Events	
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\cpeGx.bat</pre>
Creates:	<pre>C:\Documents and Settings\Admin\Application Data\Run32.exe</pre>
Creates:	<pre>C:\Documents and Settings\Admin\Application Data\cunt.exe</pre>
Creates:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\4e79_appcompat.txt</pre>
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\A61AF1.dmp
Opens:	C:\WINDOWS\Prefetch\5700C49F29B6358692EE50CB31D7A-0F4B2019.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\msvbvm60.dll
Opens:	C:\WINDOWS\system32\imm32.dll
Opens:	C:\WINDOWS\system32\rpcss.dll
Opens:	C:\WINDOWS\system32\MSCTF.dll
Opens:	C:\WINDOWS\system32\sxs.dll
Opens:	C:\WINDOWS\system32\MSCTFIME.IME
Opens:	C:\WINDOWS\system32\clbcatq.dll
Opens:	C:\WINDOWS\system32\comres.dll
Opens:	C:\WINDOWS\Registration\R00000000007.clb
Opens:	C:\WINDOWS\system32\scrrun.dll
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_6595b64144ccf1d	df_6.0.2600.5512_x-ww_35d4ce83
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1d	df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens:	C:\WINDOWS\WindowsShell.Manifest
Opens:	C:\WINDOWS\WindowsShell.Config
Opens:	C:\WINDOWS\system32\comctl32.dll
Opens:	C:\WINDOWS\system32\comctl32.dll.124.Manifest
Opens:	C:\WINDOWS\system32\comctl32.dll.124.Config
Opens:	C:\WINDOWS\system32\netapi32.dll
Opens:	C:\WINDOWS\system32\setupapi.dll
Opens:	C:\
Opens:	C:\Documents and Settings
Opens:	C:\Documents and Settings\Admin\My Documents\desktop.ini
Opens:	C:\Documents and Settings\All Users
Opens:	C:\Documents and Settings\All Users\Documents\desktop.ini
Opens:	C:\WINDOWS\system32\urlmon.dll
Opens:	C:\WINDOWS\system32\urlmon.dll.123.Manifest
Opens:	C:\WINDOWS\system32\urlmon.dll.123.Config
Opens:	C:\Documents and Settings\Admin\Local Settings
Opens:	C:\Documents and Settings\Admin\Local Settings\Temp
Opens:	<pre>C:\Documents and Settings\Admin\Local Settings\Temp\cpeGx.bat</pre>
Opens:	C:\WINDOWS\system32\apphelp.dll
Opens:	C:\WINDOWS\AppPatch\sysmain.sdb
Opens:	C:\WINDOWS\AppPatch\systest.sdb
Opens:	C:\WINDOWS\system32\cmd.exe
Opens:	C:\WINDOWS\system32\cmd.exe.Manifest
Opens:	C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf
Opens:	C:
Opensi	C. MITADONIC

C:\WINDOWS\AppPatch Opens: Opens: C:\WINDOWS\system32 C:\WINDOWS\system32\wbem Opens: Opens: C:\WINDOWS\WinSxS Opens: C:\WINDOWS\system32\ntdll.dll Opens: C:\WINDOWS\system32\kernel32.dll Opens: C:\WINDOWS\system32\unicode.nls Opens: C:\WINDOWS\system32\locale.nls Opens: C:\WINDOWS\system32\sorttbls.nls Opens: C:\WINDOWS\system32\msvcrt.dll Opens: C:\WINDOWS\system32\user32.dll Opens: C:\WINDOWS\system32\gdi32.dll Opens: C:\WINDOWS\system32\shimeng.dll Opens: C:\WINDOWS\AppPatch\AcGenral.dll Opens: C:\WINDOWS\system32\advapi32.dll C:\WINDOWS\system32\rpcrt4.dll Opens: Opens: C:\WINDOWS\system32\secur32.dll Opens: C:\WINDOWS\system32\winmm.dll Opens: C:\WINDOWS\system32\ole32.dll Opens: C:\WINDOWS\system32\oleaut32.dll Opens: C:\WINDOWS\system32\msacm32.dll Opens: C:\WINDOWS\system32\version.dll Opens: C:\WINDOWS\system32\shlwapi.dll Opens: C:\WINDOWS\system32\userenv.dll Opens: C:\WINDOWS\system32\uxtheme.dll Opens: C:\WINDOWS\system32\ctype.nls Opens: C:\WINDOWS\system32\sortkey.nls Opens: C:\WINDOWS\system32\wbem\wmic.exe C:\WINDOWS\system32\reg.exe Opens: Opens: C:\WINDOWS\system32\reg.exe.Manifest Opens: C:\WINDOWS\Prefetch\REG.EXE-0D2A95F7.pf Opens: C:\WINDOWS\system32\SHELL32.dll.124.Manifest Opens: C:\WINDOWS\system32\SHELL32.dll.124.Config Opens: C:\WINDOWS\Temp\5700c49f29b6358692ee50cb31d7ad54.exe Opens: C:\Documents and Settings\Admin\Application Data Opens: C:\Documents and Settings\Admin\Application Data\Run32.exe Opens: C:\Documents and Settings\Admin\Application Data\Run32.exe.Manifest C:\WINDOWS\Prefetch\RUN32.EXE-1311A92B.pf Opens: Opens: C:\WINDOWS\WINHELP.INI Opens: C:\Documents Opens: C:\Documents and Opens: C:\Documents and Settings\Admin\Application Opens: C:\WINDOWS\system32\ws2\_32.dll Opens: C:\WINDOWS\system32\ws2help.dll Opens: C:\WINDOWS\system32\psapi.dll Opens: C:\WINDOWS\system32\WININET.dll.123.Manifest C:\WINDOWS\system32\WININET.dll.123.Config Opens: Opens: C:\Documents and Settings\Admin\Application Data\cunt.exe Opens: C:\WINDOWS\Temp\73a92a48-b354-4263-bcb0-807e6f3d1e6b  ${\tt C:\WINDOWS\system32\mswsock.dll}$ Opens: Opens: C:\WINDOWS\system32\dnsapi.dll Opens: C:\WINDOWS\system32\winrnr.dll C:\WINDOWS\system32\drivers\etc\hosts Opens: Opens: C:\WINDOWS\system32\rsaenh.dll Opens: C:\WINDOWS\system32\hnetcfg.dll Opens: C:\WINDOWS\system32\wshtcpip.dll Opens: C:\WINDOWS\system32\rasadhlp.dll Opens: C:\WINDOWS\system32\calc.exe Opens: C:\WINDOWS\system32\faultrep.dll Opens: C:\WINDOWS\system32\wininet.dll Opens: C:\WINDOWS\system32\winsock.dll Opens: C:\Documents and Settings\Admin\Local Settings\Temp\4e79\_appcompat.txt Opens: C:\WINDOWS\system32\dwwin.exe Opens: C:\WINDOWS\system32\dwwin.exe.Manifest Opens: C:\WINDOWS\Prefetch\DWWIN.EXE-30875ADC.pf Opens: C:\WINDOWS\system32\1033 Opens: C:\WINDOWS\system32\en-US Opens: C:\WINDOWS\system32\iertutil.dll Opens: C:\WINDOWS\system32\normaliz.dll Opens: C:\WINDOWS\system32\win32k.sys C:\WINDOWS\system32\riched20.dll Opens: Opens: C:\WINDOWS\system32\shfolder.dll Opens: C:\WINDOWS\system32\1033\dwintl.dll Opens: C:\WINDOWS\system32\en-US\wininet.dll.mui Opens: C:\WINDOWS\system32\rasapi32.dll Opens: C:\WINDOWS\system32\rasman.dll C:\WINDOWS\system32\tapi32.dll Opens: Opens: C:\WINDOWS\system32\rtutils.dll Opens: C:\WINDOWS\system32\sensapi.dll Opens: C:\WINDOWS\system32\msv1\_0.dll

Opens: C:\WINDOWS\win.ini
Opens: C:\WINDOWS\system32\oleacc.dll

C:\WINDOWS\system32\iphlpapi.dll

Opens:

```
C:\WINDOWS\system32\msvcp60.dll
 Opens:
 Opens:
                          C:\WINDOWS\system32\oleaccrc.dll
 Opens:
                          C:\WINDOWS\svstem32\narrhook.dll
 Opens:
                          C:\WINDOWS\system32\COMCTL32.DLL.124.Manifest
 Opens:
                          C:\WINDOWS\system32\COMCTL32.DLL.124.Config
 Opens:
                          C:\WINDOWS\system32\SHELL32.DLL.124.Manifest
 Opens:
                          C:\WINDOWS\system32\SHELL32.DLL.124.Config
                          C:\WINDOWS\system32\URLMON.DLL.123.Manifest
 Opens:
 Opens:
                          C:\WINDOWS\system32\URLMON.DLL.123.Config
 Opens:
                          C:\WINDOWS\system32\WININET.DLL.123.Manifest
 Opens:
                          C:\WINDOWS\system32\WININET.DLL.123.Config
 Opens:
                          C:\WINDOWS\explorer.exe
 Opens:
                          C:\WINDOWS\system32\browseui.dll
 Opens:
                          C:\WINDOWS\system32\shdocvw.dll
 Opens:
                          C:\WINDOWS\system32\crypt32.dll
 Opens:
                          C:\WINDOWS\system32\msasn1.dll
 Opens:
                          C:\WINDOWS\system32\cryptui.dll
 Opens:
                          C:\WINDOWS\system32\wintrust.dll
 Opens:
                          C:\WINDOWS\system32\imagehlp.dll
 Opens:
                          C:\WINDOWS\system32\wldap32.dll
 Opens:
                          C:\WINDOWS\system32\cscui.dll
 Opens:
                          C:\WINDOWS\system32\cscdll.dll
 Opens:
                          C:\WINDOWS\system32\themeui.dll
 Opens:
                          C:\WINDOWS\system32\msimg32.dll
 Opens:
                          C:\WINDOWS\system32\xpsp2res.dll
 Opens:
                          C:\WINDOWS\system32\actxprxy.dll
 Opens:
                          C:\WINDOWS\system32\msutb.dll
 Opens:
                          C:\WINDOWS\system32\msi.dll
                          C:\WINDOWS\system32\ieframe.dll
 Opens:
 Opens:
                          C:\WINDOWS\system32\ntshrui.dll
 Opens:
                          C:\WINDOWS\system32\atl.dll
 Opens:
                          C:\WINDOWS\system32\winsta.dll
 Opens:
                          C:\WINDOWS\system32\webcheck.dll
 Opens:
                          C:\WINDOWS\system32\mlang.dll
 Opens:
                          C:\WINDOWS\system32\stobject.dll
 Opens:
                          C:\WINDOWS\system32\batmeter.dll
 Opens:
                          C:\WINDOWS\system32\powrprof.dll
 Opens:
                          C:\WINDOWS\system32\wtsapi32.dll
 Opens:
                          C:\WINDOWS\system32\netshell.dll
 Opens:
                          C:\WINDOWS\system32\credui.dll
 Opens:
                          C:\WINDOWS\system32\dot3api.dll
 Opens:
                          C:\WINDOWS\system32\dot3dlg.dll
 Opens:
                          C:\WINDOWS\system32\onex.dll
                          C:\WINDOWS\system32\eappcfg.dll
 Opens:
 Opens:
                          C:\WINDOWS\system32\eappprxy.dll
 Opens:
                          C:\WINDOWS\system32\mpr.dll
                          C:\WINDOWS\system32\drprov.dll
 Opens:
 Opens:
                          C:\WINDOWS\system32\ntlanman.dll
 Opens:
                          C:\WINDOWS\system32\netui0.dll
 Opens:
                          C:\WINDOWS\system32\netui1.dll
 Opens:
                          C:\WINDOWS\system32\netrap.dll
 Opens:
                          C:\WINDOWS\system32\samlib.dll
 Opens:
                          C:\WINDOWS\system32\davclnt.dll
 Opens:
                          C:\WINDOWS\system32\MSIMTF.dll
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\Temp\A61AF1.dmp
                          {\tt C:\Documents\ and\ Settings\setminus Admin\setminus Local\ Settings\setminus Temporary\ Internet\ Files}
 Opens:
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5
                          C:\Documents and Settings\Admin\Local Settings\History
 Opens:
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\History\History.IE5
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
                          C:\Documents and Settings\Admin\Cookies
 Opens:
                          C:\Documents and Settings\Admin\Cookies\index.dat
                          C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\index.dat
 Opens:
                          C:\WINDOWS\system32\TAPI32.dll.124.Manifest
                          C:\WINDOWS\system32\TAPI32.dll.124.Config
 Opens:
 Opens:
                          C:\AUTOEXEC.BAT
 Opens:
                          C:\Documents and Settings\All Users\Application
{\tt Data\Microsoft\Network\Connections\Pbk}
                          C:\WINDOWS\system32\ras
 Opens:
 Opens:
                          C:\Documents and Settings\Admin\Application
Data\Microsoft\Network\Connections\Pbk\
 Opens:
                          C:\WINDOWS\Fonts\sserife.fon
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temp\cpeGx.bat
 Writes to:
                          C:\Documents and Settings\Admin\Application Data\Run32.exe
 Writes to:
                          C:\Documents and Settings\Admin\Application Data\cunt.exe
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temp\4e79_appcompat.txt
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\A61AF1.dmp}
 Writes to:
 Reads from:
                          C:\WINDOWS\Registration\R00000000007.clb
 Reads from:
                          C:\WINDOWS\system32\scrrun.dll
```

C:\Documents and Settings\Admin\My Documents\desktop.ini

Reads from:

Reads from: C:\Documents and Settings\All Users\Documents\desktop.ini Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\cpeGx.bat C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf Reads from: Reads from: C:\WINDOWS\Temp\5700c49f29b6358692ee50cb31d7ad54.exe

Reads from: C:\Documents and Settings\Admin\Application Data\Run32.exe Reads from: C:\WINDOWS\system32\drivers\etc\hosts

Reads from: C:\WINDOWS\system32\rsaenh.dll Reads from: C:\WINDOWS\system32\calc.exe Reads from: C:\WINDOWS\system32\winsock.dll

C:\WINDOWS\Prefetch\DWWIN.EXE-30875ADC.pf Reads from:

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

Deletes: C:\Documents and Settings\Admin\Application Data\Run32.exe

#### Network Events

DNS query: xdanx.dyndns.org

DNS response:  $xdanx.dyndns.org \Rightarrow 184.169.144.229$ 

184.169.144.229:9872 Connects to:

Sends data to: 8.8.8.8:53

Sends data to: xdanx.dyndns.org:9872 (184.169.144.229)

Receives data from: 0.0.0.0:0

Receives data from: xdanx.dyndns.org:9872 (184.169.144.229)

#### Windows Registry Events

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

folders

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

Creates key:

806d6172696f}\

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

folders

 $\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in \begin{tabular}{ll} windows \end{tabular} current version \end{tabular} explorer \end{tabular} software \end{tabular} in \begin{tabular}{ll} windows \end{tabular} current version \end{tabular} explorer \end{tabular} software \end{tabular} in \begin{tabular}{ll} windows \end{tabular} explorer \end{tabular} explorer \end{tabular} software \end{tabular} explorer \end{$ Creates key:

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

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

v4.00

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

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

HKCU\software Creates key:

HKCU\software\microsoft Creates key:

HKCU\software\microsoft\visual basic Creates kev:

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

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

Creates key: HKCU\sessioninformation

HKLM\software\microsoft\pchealth\errorreporting Creates key:

Creates key: HKLM\software\microsoft\pchealth\errorreporting\exclusionlist Creates key:  $\label{lem:hklm} \verb+KKLM\software\microsoft\pchealth\errorreporting\nclusion list$ 

Creates key: HKLM\software\microsoft\tracing

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

settings\connections

Deletes value: HKLM\software\microsoft\pchealth\errorreporting\dw[dwfiletreeroot]

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

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

options\5700c49f29b6358692ee50cb31d7ad54.exe

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

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

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

options\gdi32.dll

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

options\user32.dll

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

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

options\imm32.dll

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

options\ntdll.dll

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

options\kernel32.dll

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

options\secur32.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rpcrt4.dll

Opens kev:

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

options\advapi32.dll

Opens key:

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

Opens key:

options\ole32.dll

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

Opens key:

options\oleaut32.dll

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

Opens key:

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

options\msvbvm60.dll

Opens key: HKLM\system\currentcontrolset\control\error message instrument\ Opens key: HKLM\system\currentcontrolset\control\error message instrument HKLM\software\microsoft\windows nt\currentversion\gre\_initialize Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32 Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility

HKI M\software\microsoft\windows nt\currentversion\windows Opens kev: Opens key: HKLM\software\microsoft\windows nt\currentversion\winlogon

Opens key: HKLM\

 $\label{thm:local_hammon} \mbox{HKLM\software\mbox{\sc microsoft\windows} nt\current version\diagnostics} \\$ Opens key:

Opens key: HKLM\software\microsoft\ole

Opens key: HKCR\interface

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

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

Opens key: HKCU\

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

Opens key: HKCU\control panel\desktop

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

options\msctf.dll

Opens key:

HKLM\software\microsoft\ctf\compatibility\5700c49f29b6358692ee50cb31d7ad54.exe

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

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

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

options\sxs.dll

Opens key: HKLM\system\setup

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

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

options\version.dll

Opens key:  $\label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\windows} nt\current\version\app\compatflags\layers} \\$ Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msctfime.ime

Opens key: HKCU\software\microsoft\ctf

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

 ${\tt HKLM \ } system \verb|\ current control \ \\ set \verb|\ control \ \\ nls \verb|\ codepage \ \\$ Opens key:

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

Opens kev: HKLM\software\microsoft\com3  $\label{lem:hklm} \verb+Kklm \+ software + microsoft + windows nt + current version + image file execution$ Opens key:

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

Opens key:

options\clbcatq.dll HKLM\software\microsoft\com3\debug Opens key:

Opens key: HKCU\software\classes\ HKLM\software\classes Opens key:

Opens key: HKU\ Opens key: HKCR\clsid

HKCU\software\classes\scripting.filesystemobject Opens key:

Opens key: HKCR\scripting.filesystemobject

Opens key: HKCU\software\classes\scripting.filesystemobject\clsid

Opens key:  ${\tt HKCR\backslash scripting.filesystemobject\backslash clsid}$ 

Opens key:  $HKCU \setminus software \setminus classes \setminus clsid \setminus \{0d43fe01 - f093 - 11cf - 8940 - 00a0c9054228\}$ 

Opens key: HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228} Opens key:

00a0c9054228}\treatas

Opens key: HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\treatas HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-Opens key:

00a0c9054228}\inprocserver32

HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\inprocserver32 Opens kev:

Opens key: HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-

00a0c9054228}\inprocserverx86

Opens key: HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\inprocserverx86

HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-Opens key:

00a0c9054228}\localserver32

HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\localserver32 Opens kev:

Opens key: HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-

00a0c9054228}\inprochandler32

Opens key: HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\inprochandler32

Opens key: HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-

00a0c9054228}\inprochandlerx86

HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\inprochandlerx86 Opens key:

Opens key: HKCU\software\classes\clsid\{0d43fe01-f093-11cf-894000a0c9054228}\localserver

HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\localserver Opens kev:

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

options\scrrun.dll

Opens key: HKCU\software\classes\typelib

Opens key: HKCR\typelib

HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-00a0c9054228} Opens key:

HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228} Opens key:

HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0 Opens key:

HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0 Opens key: Opens key: HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-

00a0c9054228}\1.0\0

Opens key: HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0 HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-Opens key:

00a0c9054228}\1.0\0\win32

HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0\win32 Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\shlwapi.dll

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

options\shell32.dll Opens key:

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

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

options\comctl32.dll

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

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

options\netapi32.dll

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

Opens key: HKLM\software\microsoft\rpc

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

options\5700c49f29b6358692ee50cb31d7ad54.exe\rpcthreadpoolthrottle Opens key: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKLM\system\currentcontrolset\control\computername

HKLM\system\currentcontrolset\control\computername\activecomputername Opens key: Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer

Opens key:

 $HKLM \ software \ `microsoft \ windows \ current version \ shell compatibility \ applications \ 5700c49f29b6358692ee50cb31d7ad54.exe$ Opens key:

HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{20d04fe0-3aea-1069-

a2d8-08002b30309d}

Opens key:

08002b30309d}\inprocserver32

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

HKCU\software\classes\drive\shellex\folderextensions Opens kev: HKCR\drive\shellex\folderextensions

Opens key:

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

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

4442-804e-409d6c4515e9}

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

409d6c4515e9}

Opens kev: HKCU\software\microsoft\windows\currentversion\explorer\fileexts  $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ fileexts\+ .bat$ Opens key:

Opens key: HKCU\software\classes\.bat

Opens key: HKCR\.bat

HKCU\software\classes\batfile Opens key:

Opens key: HKCR\batfile

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

HKCR\batfile\curver Opens key:

Opens key: HKCR\batfile\

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

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

Opens key: HKCR\batfile\shellex\iconhandler

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

Opens key: HKCR\systemfileassociations\.bat

Opens key: HKCU\software\classes\systemfileassociations\application

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

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

Opens key: HKCR\\*

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

HKCR\\*\clsid Opens key:

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

options\setupapi.dll

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

Opens key: HKLM\system\wpa\pnp

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

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

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key: HKLM\software\policies\microsoft\system\dnsclient
Opens key:

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

Opens key:

11e3-9fc7-806d6172696f}\

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

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

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

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

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

Opens key: HKCR\directory\clsid
Opens key: HKCU\software\classes\folder

Opens key: HKCR\folder

Opens key: HKCU\software\classes\folder\clsid

Opens key: HKCR\folder\clsid

Opens key:

HKLM\software\microsoft\windows\currentversion\explorer\shellexecutehooks
Opens key: HKCU\software\classes\clsid\{aeb6717e-7e19-11d0-97ee-

00c04fd91972}\inprocserver32

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

Opens key: HKCU\software\classes\.ade

Opens key: HKCR\.ade

Opens key: HKCU\software\classes\.adp

Opens key: HKCR\.adp

Opens key: HKCU\software\classes\.app

Opens key: HKCR\.app

Opens key: HKCU\software\classes\.asp

Opens key: HKCR\.asp

Opens key: HKCU\software\classes\.bas

Opens key: HKCR\.bas

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

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

00c04fb6bfc4}\treatas

 $00c04fb6bfc4\\ \\ \\ inprocserver32$ 

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

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

00c04fb6bfc4}\inprocserverx86

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

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

 $00c04fb6bfc4\\ \\ \\ local server 32$ 

 $Opens~key: \\ HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver 32$ 

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

00c04fb6bfc4}\inprochandler32

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

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

00c04fb6bfc4}\inprochandlerx86

 $Opens~key: \\ HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\ \ inprochandlerx86$ 

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

00c04fb6bfc4}\localserver

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

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

options\iertutil.dll

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

options\urlmon.dll

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

Opens key: HKCR\protocols\name-space handler

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

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

settings

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

settings
 Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature\_protocol\_lockdown
 Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature\_protocol\_lockdown

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

settings\

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

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

```
Opens key:
                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
 Opens key:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
 Opens kev:
                           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\currentversion\internet
settings\zonemap\ranges\
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\zonemap\ranges\
 Opens key:
                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
 Opens key:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
 Opens kev:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
 Opens key:
                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
 Opens key:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
 Opens kev:
                           HKLM\software\policies
 Opens key:
                           HKCU\software\policies
 Opens key:
                           HKCU\software
                          HKLM\software
 Opens key:
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Opens kev:
settings\zonemap\protocoldefaults\
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
                           HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus internet
 Opens key:
settings\zonemap\domains\
                          HKLM\software\microsoft\windows\currentversion\internet
 Opens key:
settings\zonemap\domains\msn.com
                          HKLM\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\zonemap\domains\msn.com\related
                           HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
                          HKCU\software\microsoft\internet explorer\ietld
 Opens kev:
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
                          HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature http username password disable
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
                          HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
 Opens key:
                           HKLM\software\policies\microsoft\internet explorer
 Opens key:
                           HKLM\software\policies\microsoft\internet explorer\security
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\
 Opens key:
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
 Opens key:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
 Opens key:
                           \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\zones\0
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
 Opens key:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
 Opens key:
                           \label{lem:hkcu} \verb+KCU\+software\+policies\+microsoft\+windows\+currentversion\+internet
settings\zones\1
 Opens key:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\zones\2
 Opens key:
                           \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\zones\3
 Opens key:
                           \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
```

```
settings\zones\3
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\zones\4
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
                          HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
 Opens key:
                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
settings\lockdown_zones\
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\0
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\1
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\1
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\2
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\2
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\2
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\3
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\4
                          \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
 Opens key:
settings\lockdown_zones\4
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
                          HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
 Opens key:
                          HKCU\software\classes\batfile\shell
                          HKCR\batfile\shell
 Opens kev:
 Opens key:
                          HKCU\software\classes\batfile\shell\open
 Opens key:
                          HKCR\batfile\shell\open
                          HKCU\software\classes\batfile\shell\open\command
 Opens key:
                          HKCR\batfile\shell\open\command
 Opens kev:
 Opens key:
\label{thm:local_hammon_hammon} \begin{tabular}{l} HKCU \software \mbox{$\mbox{$m$icrosoft}$ windows \current version \policies \explorer \restrict run \end{tabular}
                          HKLM\software\microsoft\windows\currentversion\app paths\cpegx.bat
 Opens kev:
 Opens key:
                          HKCU\software\classes\batfile\shell\open\ddeexec
 Opens key:
                          HKCR\batfile\shell\open\ddeexec
 Opens key:
                          HKCU\software\classes\applications\cpegx.bat
 Opens key:
                          HKCR\applications\cpegx.bat
 Opens key:
                          HKCU\software\microsoft\windows\shellnoroam
 Opens key:
                          HKCU\software\microsoft\windows\shellnoroam\muicache
                          HKCU\software\microsoft\windows\shellnoroam\muicache\
 Opens key:
 Opens key:
                          HKLM\software\microsoft\windows\currentversion\explorer\fileassociation
 Opens key:
                          HKLM\system\currentcontrolset\control\session manager\appcompatibility
 Opens key:
                          \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution
options\apphelp.dll
 Opens kev:
                          HKLM\svstem\wpa\tabletpc
 Opens key:
                          HKLM\system\wpa\mediacenter
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
 Opens key:
                          HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\cpegx.bat
 Opens key:
                          HKLM\software\policies\microsoft\windows\safer\levelobjects
 Opens kev:
                          HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
 Opens key:
```

be2efd2c1a33} Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes

Opens key:

edd5fbde1328}

Opens key:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{7fb9cd2e-3076-4df9-a57b-4df9-a57$ b813f72dbb91}

Opens key:

7c29ddecae3f}

Opens key:

085bcc18a68d}

Opens key:

b91490411bfc}

Opens key:

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

Opens key:

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

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes 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 kev:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes 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\codeidentifiers\131072\paths Opens kev:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus hashes$ Opens kev:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths Opens kev:

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

Opens kev:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus urlzones$ 

 $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus paths$ Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes Opens key: Opens key:

 $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus urlzones$ Opens kev:

 $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus paths$ Opens kev: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes

Opens key:  $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus urlzones$ 

Opens kev: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths

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

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \code ident$ Opens kev:

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

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

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

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

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

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

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\cmd.exe

Opens key: HKCU\software\policies\microsoft\windows\system Opens key: HKLM\software\microsoft\command processor Opens key: HKCU\software\microsoft\command processor Opens key: HKLM\system\currentcontrolset\control\nls\locale

Opens key:  $HKLM \ system \ current controls et \ control \ nls \ locale \ alternate \ sorts$ 

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

Opens key: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags\custom\reg.exe

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

options\reg.exe

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

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

options\shimeng.dll

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

options\winmm.dll

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

options\msacm32.dll

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

options\userenv.dll

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

options\uxtheme.dll

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

Opens key:

HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache

Opens key:

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

Opens key:

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

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

Opens key:

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

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

Opens key:

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

Opens kev:

 $HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus msacm. sl\_anet$ 

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

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

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

folders

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

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

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

Opens key: HKCU\software\classes\.exe

Opens key: HKCR\.exe

Opens key: HKCU\software\classes\exefile

Opens key: HKCR\exefile

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

Opens key: HKCR\exefile\curver
Opens key: HKCR\exefile\

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

Opens key: HKCR\exefile\shellex\iconhandler

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

Opens key: HKCR\systemfileassociations\.exe
Opens key: HKCU\software\classes\exefile\clsid

Opens key: HKCR\exefile\clsid

Opens key: HKCU\software\classes\.cer

Opens key: HKCR\.cer

Opens key: HKCU\software\classes\.chm

Opens key: HKCR\.chm

Opens key: HKCU\software\classes\.cmd

Opens key: HKCR\.cmd

Opens key: HKCU\software\classes\.com

Opens key: HKCR\.com

Opens key: HKCU\software\classes\.cpl
Opens key: HKCR\.cpl

Opens key: HKCU\software\classes\.crt
Opens key: HKCR\.crt
Opens key: HKCU\software\classes\.csh

Opens key: HKCR\.csh

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

Opens key: HKCR\exefile\shell

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

Opens key: HKCR\exefile\shell\open

Opens key:  $\label{log:hkcu} \mbox{HKCU\software\classes\exefile\shell\open\command} \\$ 

Opens key:  ${\tt HKCR} \verb| exefile \verb| shell \verb| open \verb| command |$ 

 $Opens\ key: \\ HKLM\software\microsoft\windows\currentversion\app\ paths\run32.exe$ 

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

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

Opens key: HKCU\software\classes\applications\run32.exe

Opens key: HKCR\applications\run32.exe
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\run32.exe

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

options\run32.exe

Opens key: HKLM\software\microsoft\windows

Opens key: HKLM\software\microsoft\windows\html help
Opens key: HKLM\software\microsoft\windows\help

Opens key: HKLM\software\microsoft\ctf\compatibility\run32.exe

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ws2help.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ws2\_32.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: options\normaliz.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wininet.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\psapi.dll Opens key: HKLM\svstem\currentcontrolset\control\wmi\security Opens key:  $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \crossft \color= \color= \crossft \crossft \color= \crossft \color= \crossft \color= \crossft \color= \crossft \color= \crossft \crossft \color= \crossft \color= \crossft \crossft \color= \crossft \crossf$ Opens key: HKLM\software\microsoft\windows\currentversion\run  $\label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ services \+ winsock 2 \+ parameters$ Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\00000004 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000001 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000000 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000004 Opens kev: Opens kev: Opens key: Opens key: Opens kev: Opens key:  $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ (catalog\_entries \ 000000000010) \ (catalog\_entries \ (catalog \ (catalog\_entries \ (catalog \ (catal$ Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\00000004 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001 Opens kev: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000003 HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\mswsock.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dnsapi.dll Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient Opens key: c7d49d7cecdc} Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution options\winrnr.dll Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rsaenh.dll Opens kev: HKLM\software\policies\microsoft\cryptography Opens key: HKLM\software\microsoft\cryptography Opens key: HKLM\software\microsoft\cryptography\offload Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\hnetcfg.dll Opens key: HKLM\software\microsoft\rpc\securityservice Opens kev: HKLM\svstem\currentcontrolset\services\winsock\parameters Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wshtcpip.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

Opens key: HKCU\software\classes\applications\calc.exe
Opens key: HKCR\applications\calc.exe

options\rasadhlp.dll

```
Opens key:
                                                         HKLM\software\microsoft\ctf\tip\
   Opens key:
                                                         HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}
   Opens key:
                                                         HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}
   Opens key:
                                                         HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
c9633f71be64}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}
                                                         HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
   Opens key:
77e8f3d1aa80}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}
   Opens key:
                                                         HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
   Opens key:
                                                         HKLM \setminus software \setminus microsoft \setminus tip \setminus \{78cb5b0e-26ed-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fc
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
   Opens key:
                                                         HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
   Opens key:
                                                         HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
   Opens key:
                                                         HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}
                                                         HKLM \setminus software \setminus microsoft \setminus tip \setminus \{78cb5b0e-26ed-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fc
   Opens key:
77e8f3d1aa80}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}
                                                         HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
   Opens key:
c9633f71be64}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
   Opens key:
                                                         HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
                                                         HKLM\software\microsoft\windows nt\currentversion\aedebug
   Opens key:
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\faultrep.dll
   Opens key:
                                                         HKLM\software\policies\microsoft\pchealth\errorreporting
   Opens key:
                                                         HKLM\software\microsoft\pchealth\errorreporting\dw
   Opens key:
                                                         HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\dwwin.exe
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dwwin.exe
   Opens key:
                                                         HKCU\software\microsoft\office\10.0\common\debug
   Opens key:
                                                         HKLM\software\microsoft\oasys\oaclient
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\riched20.dll
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
options\shfolder.dll
   Opens key:
                                                         HKLM\software\microsoft\office\10.0\common\installroot
   Opens key:
                                                         HKLM\software\microsoft\ctf\compatibility\dwwin.exe
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion
   Opens key:
                                                         HKCU\software\microsoft\internet explorer\settings
   Opens key:
                                                         HKLM\software\microsoft\pchealth\errorreporting\dw\debug
   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\dwwin.exe\rpcthreadpoolthrottle
                                                         HKLM\software\policies\microsoft\internet explorer\main
   Opens kev:
   Opens key:
                                                         HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache
                                                         HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\5.0\cache
                                                         HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\5.0\cache\content
   Opens key:
                                                         HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
                                                         HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\5.0\cache\cookies
                                                         HKLM\software\microsoft\windows\currentversion\internet
   Opens key:
settings\5.0\cache\cookies
   Opens key:
                                                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
                                                         HKLM\software\microsoft\windows\currentversion\internet
   Opens kev:
settings\5.0\cache\history
                                                         HKCU\software\microsoft\windows\currentversion\internet
   Opens kev:
settings\5.0\cache\extensible cache
                                                         HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\5.0\cache\extensible cache\domstore
                                                         HKCU\software\microsoft\windows\currentversion\internet
   Opens kev:
settings\5.0\cache\extensible cache\feedplat
                                                         HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\5.0\cache\extensible cache\iecompat
   Opens key:
                                                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
   Opens kev:
                                                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407
                                                         HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\5.0\cache\extensible cache\mshist012014041220140413
   Opens key:
                                                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
                                                         HKCU\software\microsoft\internet
   Opens key:
\verb|explorer| \verb|main| feature control| retry_header on lypost\_on connection reset| \\
```

```
HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
 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
                         HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0\cache
 Opens key:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                         HKLM\software\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
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
 Opens kev:
                         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
                         HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
 Opens kev:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dwintl.dll
                         HKCU\software\microsoft\windows\currentversion\internet settings\wpad
 Opens kev:
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasman.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rtutils.dll
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens kev:
options\tapi32.dll
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\telephony
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasapi32.dll
 Opens key:
                         HKLM\software\microsoft\tracing\rasapi32
                         HKLM\software\microsoft\windows nt\currentversion\profilelist
 Opens kev:
 Opens key:
                         HKLM\system\currentcontrolset\control\session manager\environment
                         HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
 Opens key:
1757981266-507921405-1957994488-1003
 Opens key:
                         HKCU\environment
 Opens key:
                         HKCU\volatile environment
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\sensapi.dll
 Opens key:
                         HKCU\software\microsoft\windows nt\currentversion\windows
 Opens key:
                         HKLM\system\currentcontrolset\control\securityproviders
 Opens key:
                         HKLM\system\currentcontrolset\control\lsa\sspicache
 Opens key:
                         HKLM \ system \ current control \ lsa \ spicache \ msaps spc. dll
```

HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll

 $HKLM \ system \ current control \ lsa \ sspicache \ msnsspc. dll$ 

Opens kev:

Opens key:

Opens key: HKLM\system\currentcontrolset\control\securityproviders\saslprofiles HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev:

options\iphlpapi.dll

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

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

Opens key: HKLM\system\currentcontrolset\services\netbt\parameters Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msv1\_0.dll

Opens key: HKCU\appevents\schemes\apps\.default\systemnotification\.current HKLM\system\currentcontrolset\control\terminal server[tsappcompat] Oueries value:

Queries value:

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

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

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

nt\currentversion\compatibility32[5700c49f29b6358692ee50cb31d7ad54]

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

compatibility[5700c49f29b6358692ee50cb31d7ad54]

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

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

manager[criticalsectiontimeout]

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

Queries value: HKCR\interface[interfacehelperdisableall]

Queries value: HKCR\interface[interfacehelperdisableallforole32] Oueries value: HKCR\interface[interfacehelperdisabletypelib] HKCR\interface\{00020400-0000-0000-c000-Queries value:

00000000046}[interfacehelperdisableall]

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

00000000046}[interfacehelperdisableallforole32]

Queries value: HKCU\control panel\desktop[multiuilanguageid] Oueries value: HKLM\software\microsoft\ctf\systemshared[cuas] Queries value: HKCU\keyboard layout\toggle[language hotkey]

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

Oueries value: HKCU\keyboard layout\toggle[layout hotkey] HKLM\software\microsoft\ctf[enableanchorcontext] Queries value: Queries value: HKLM\system\currentcontrolset\control\session

manager[safeprocesssearchmode]

HKLM\software\microsoft\windows nt\currentversion\imm[ime file] Queries value: HKCU\software\microsoft\ctf[disable thread input manager] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\codepage[932] HKLM\system\currentcontrolset\control\nls\codepage[949] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\codepage[950] Oueries value:  $HKLM \setminus system \setminus current control \setminus nls \setminus codepage \cite{Management} \cite{Managemen$ 

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

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

HKLM\software\microsoft\com3[regdbversion] Oueries value: HKCR\scripting.filesystemobject\clsid[] Oueries value: Queries value: HKCR\clsid\{0d43fe01-f093-11cf-8940-

00a0c9054228}\inprocserver32[inprocserver32]

HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\inprocserver32[] Oueries value:

HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}[appid] Queries value:

HKCR\clsid\{0d43fe01-f093-11cf-8940-Oueries value:

00a0c9054228}\inprocserver32[threadingmodel]

HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0\win32[] Oueries value:

Queries value: HKLM\system\setup[systemsetupinprogress] HKCU\control panel\desktop[smoothscroll] Queries value:

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps] Oueries value: Queries value: HKLM\software\microsoft\windows\currentversion\explorer[maximizeapps]

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

Queries value:

 ${\tt HKLM \ } system \verb| current control \verb| set \verb| computer name \verb| active computer name \verb| [computer name]|$ 

Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nonethood] Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer] Oueries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]

Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups] Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]

Oueries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]

Queries value:  $\label{local-condition} HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\ \ inprocserver32[]$ HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-Oueries value:

409d6c4515e9}[drivemask]

Oueries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]

Oueries value: HKCR\.bat[]

Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]

Queries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate]

Oueries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[forceactivedesktopon]

Oueries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]

Oueries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]

Oueries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell]

Oueries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess]

Oueries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]

HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]

Queries value:

 $HKCU \ software \ microsoft \ windows \ \ current version \ \ explorer \ \ \ advanced \ [dont pretty path]$ Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]

HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]

Queries value:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus advanced [mapnet drvbtn]$ 

Queries value:

 $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\advanced[webview]} \\$ 

HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]

HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]

Oueries value:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced [nonetcrawling]$ 

HKCR\batfile[docobject] Oueries value: Oueries value: HKCR\batfile[browseinplace] HKCR\batfile[isshortcut] Oueries value: Queries value: HKCR\batfile[alwaysshowext] Queries value: HKCR\batfile[nevershowext]

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

folders[personal]

Queries value: HKLM\system\wpa\pnp[seed] HKLM\system\setup[osloaderpath] Oueries value: Oueries value: HKLM\svstem\setup[svstempartition]

Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]

Queries value:

HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]

Queries value:

HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]

Oueries value: HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]

HKLM\software\microsoft\windows\currentversion[devicepath] Oueries value: HKLM\software\microsoft\windows\currentversion\setup[loglevel] Queries value: Queries value: HKLM\software\microsoft\windows\currentversion\setup[logpath] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] HKLM\system\currentcontrolset\services\tcpip\parameters[domain] Queries value: Oueries value:

11e3-9fc7-806d6172696f}[data]

Queries value:

11e3-9fc7-806d6172696f}[generation]

HKCR\directory[docobject] Oueries value: Queries value: HKCR\directory[browseinplace] HKCR\directory[isshortcut] Oueries value: Oueries value: HKCR\directory[alwaysshowext] Queries value: HKCR\directory[nevershowext]

Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]

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

folders[common documents]

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

folders[desktop]

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

folders[common desktop]

Queries value:  $\label{lem:hkcr} $$ HKCR\clsid_{aeb6717e-7e19-11d0-97ee-00c04fd91972} \in \clsid_{aeb6717e-7e19-11d0-97ee-00c04fd91972} $$ inprocessor of the context of the$  Queries value: HKCR\clsid\{aeb6717e-7e19-11d0-97ee-

00c04fd91972}\inprocserver32[loadwithoutcom]

Queries value: HKCR\.asp[]

Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[]

Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[appid]

Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\inprocserver32[threadingmodel]

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

settings[disableimprovedzonecheck]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature\_protocol\_lockdown[5700c49f29b6358692ee50cb31d7ad54.exe]

Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_protocol\_lockdown[\*]

Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]

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

settings[createuricachesize]

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

settings[createuricachesize]

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

settings[enablepunycode]

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

settings[enablepunycode]

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

explorer\security[disablesecuritysettingscheck]

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

settings\zones\0[flags]

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

settings\zones\1[flags]

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

settings\zones\2[flags]

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

settings\zones\3[flags]

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

settings\zones\4[flags]

Queries value: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_localmachine\_lockdown[5700c49f29b6358692ee50cb31d7ad54.exe]

Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_localmachine\_lockdown[\*] Queries value: HKLM\software\microsoft\internet

 $\verb|explorer| a in feature control feature_local machine_lockdown[5700c49f29b6358692ee50cb31d7ad54.exe]|$ 

Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_localmachine\_lockdown[\*]

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

settings[specialfolderscachesize]

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

settings[specialfolderscachesize]

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[cache]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[cookies]

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

settings\zones\0[1806]

Queries value:

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

Queries value: HKCR\batfile\shell[]

Queries value: HKCU\software\microsoft\windows\shellnoroam\muicache[langid]

Queries value:

HKCU\software\microsoft\windows\shellnoroam\muicache[c:\docume~1\admin\locals~1\temp\cpegx.bat]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\fileassociation[cutlist]

Queries value:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \policies \explorer[inherit consolehandles] \end{tabular}$ 

Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun]
Oueries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[disallowrun]

HKCU\software\microsoft\windows\currentversion\policies\explorer[norunasinstallprompt]

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

manager\appcompatibility[disableappcompat]

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

Queries value:

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

 $Queries\ value: \\ HKLM\ software\ policies\ microsoft\ windows\ safer\ code identifiers [levels]$ 

Queries value:

be2efd2c1a33}[itemdata]

Queries value:

```
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}[saferflags]
 Queries value:
```

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

b813f72dbb91}[hashalg]

Queries value:

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

Queries value:

b813f72dbb91}[saferflags]

Queries value:

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

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

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

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes \setminus \{81d1fe15 - dd9d - 4762 - b16d - b1$ 7c29ddecae3f}[saferflags]

Queries value:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes \setminus \{94e3e076-8f53-42a5-8411-144a6\} \setminus \{94e3e076-8f53-42a5-8414\} \setminus \{94e3e076-8f53-42a5-8414\} \setminus \{94e3e076-8f53-42a5-8414\} \setminus \{94e3e076-8f53-42a5-8414\} \setminus \{94e3e076-8f53-42a5-8414\} \setminus \{94e3e076-8f53-8644\} \setminus \{94e3e076-8646\} \setminus \{94e3e076-8646\} \setminus \{94e3e076-8646\} \setminus \{94e3e076-8646\} \setminus \{94e$ 085bcc18a68d}[itemdata]

Queries value:

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

Oueries value:

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

Queries value:

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

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

Queries value:

b91490411bfc}[hashalg]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

HKCU\software\microsoft\windows\currentversion\explorer\shell Queries value: folders[cache] Queries value:

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

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

HKLM\software\microsoft\command processor[disableunccheck] Oueries value: Queries value: HKLM\software\microsoft\command processor[enableextensions] Queries value: HKLM\software\microsoft\command processor[delayedexpansion] Oueries value: HKLM\software\microsoft\command processor[defaultcolor] Queries value: HKLM\software\microsoft\command processor[completionchar] Queries value: HKLM\software\microsoft\command processor[pathcompletionchar]

HKLM\software\microsoft\command processor[autorun] Oueries value:

Queries value: HKCU\software\microsoft\command processor[disableunccheck] Queries value: HKCU\software\microsoft\command processor[enableextensions] Oueries value: HKCU\software\microsoft\command processor[delayedexpansion] Queries value: HKCU\software\microsoft\command processor[defaultcolor]

```
Oueries value:
                                   HKCU\software\microsoft\command processor[completionchar]
                                   HKCU\software\microsoft\command processor[pathcompletionchar]
  Oueries value:
  Oueries value:
                                   HKCU\software\microsoft\command processor[autorun]
  Queries value:
                                   HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\compatibility32[reg]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\ime compatibility[reg]
  Oueries 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]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
  Oueries value:
  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]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
  Oueries value:
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
  Oueries value:
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
  Queries value:
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
  Oueries value:
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
  Queries value:
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
  Oueries value:
  Oueries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
  Oueries value:
                                   HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [mixer 1]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer31
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
  Oueries value:
                                   HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [mixer 7]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
  Oueries value:
  Queries value:
                                   HKCU\software\microsoft\multimedia\audio[systemformats]
                                   HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\drivers32[msacm.imaadpcm]
  Queries value:
Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags]
  Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[aformattagcache]
  Oueries value:
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. im a adpcm [cfilter tags]
                                  HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\drivers32[msacm.msadpcm]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[fdwsupport]
  Oueries value:
Queries value:
HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} which is a consistent with the lemma constraints of the l
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cfiltertags]
  Queries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msg711]
  Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[fdwsupport]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cformattags]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[aformattagcache]
  Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cfiltertags]
                                  HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\drivers32[msacm.msgsm610]
  Queries value:
```

```
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[fdwsupport]
     Oueries value:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. msgsm610[cformattags]
     Queries value:
HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} which is a simple that the lemma simple that th
     Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cfiltertags]
     Oueries value:
                                                                         HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.trspch]
     Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport]
     Queries value:
HKLM \label{lem:hklm} Which is a constant and incompression manager \label{lem:hklm} driver cache \label{lem:hklm} which is a constant and incompression manager \label{lem:hklm} driver cache \label{lem:hklm} which is a constant and incompression manager \label{lem:hklm} driver cache \label{lem:hklm} which is a constant and incompression manager \label{lem:hklm} driver cache \label{lem:hklm} which is a constant and incompression manager \label{lem:hklm} driver \label{lklm} driver \lab
     Oueries value:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.trspch[aformattagcache]
     Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cfiltertags]
                                                                         HKLM\software\microsoft\windows
     Queries value:
nt\currentversion\drivers32[msacm.msg723]
     Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[fdwsupport]
     Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cformattags]
Queries value:
HKLM \verb|\software\microsoft\audiocompressionmanager\drivercache\mbox{|} msg723[cfiltertags]|
                                                                         HKLM\software\microsoft\windows
     Queries value:
nt\currentversion\drivers32[msacm.msaudio1]
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[fdwsupport]
     Queries value:
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msaudio1[cformattags]
     Queries value:
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msaudio 1 [a formattag cache]
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cfiltertags]
     Queries value:
                                                                         HKLM\software\microsoft\windows
 nt\currentversion\drivers32[msacm.sl_anet]
     Queries value:
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. sl\_anet \ [fdw support]
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl anet[cformattags]
     Queries value:
HKLM \ "software\ "microsoft\ "audiocompression manager\ "drivercache\ "msacm.sl\_anet[aformattag cache]" and "msacm.sl\_anet" and "msacm.sl\_anet"
     Queries value:
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. sl\_anet [cfilter tags]
     Queries value:
                                                                         HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2]
     Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport]
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cformattags]
     Queries value:
Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cfiltertags]
     Oueries value:
                                                                         HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.l3acm]
     Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.13acm[fdwsupport]
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cformattags]
     Queries value:
Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags]
                                                                         HKCU\software\microsoft\multimedia\audio compression
     Oueries value:
manager\msacm[nopcmconverter]
     Queries value:
                                                                         \label{lem:hkcu} \verb+KKCU\software\microsoft\multimedia\audio compression manager\microsoft\multimedia\audio compression manager\microsoft\multimedia\audio compression manager\microsoft\multimedia\audio compression manager\microsoft\multimedia\audio compression manager\microsoft\multimedia\audio compression manager\microsoft\multimedia\audio compression manager\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\mi
 v4.00[priority1]
                                                                         HKLM\software\microsoft\windows
     Oueries value:
nt\currentversion\winlogon[userenvdebuglevel]
                                                                        HKLM\software\microsoft\windows
     Oueries value:
nt\currentversion\winlogon[chkaccdebuglevell
     Queries value:
                                                                        HKLM\system\currentcontrolset\control\productoptions[producttype]
     Queries value:
                                                                         HKCU\software\microsoft\windows\currentversion\explorer\user shell
 folders[local settings]
     Queries value:
                                                                         HKLM\software\microsoft\windows
 nt\currentversion\winlogon[rsopdebuglevel]
                                                                         HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
     Oueries value:
     Oueries value:
                                                                         HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
     Queries value:
                                                                         HKCU\control panel\desktop[lamebuttontext]
                                                                         \label{lem:hkcu} \verb+KKCU \software \verb+microsoft + windows + current version + run [run 32.dll]
     Oueries value:
     Queries value:
                                                                         HKCR\.exe[]
```

Oueries value: HKCR\exefile[docobject] HKCR\exefile[browseinplace] Oueries value: Oueries value: HKCR\exefile[isshortcut] Queries value: HKCR\exefile[alwaysshowext] Oueries value: HKCR\exefile[nevershowext] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[comparejunctionness] Oueries value: HKCR\.cer[] Oueries value: HKCR\.chm[] Queries value: HKCR\.cmd[] HKCR\.com[] Oueries value: Queries value: HKCR\.cpl[] Oueries value: HKCR\.crt[] Oueries value: HKCR\exefile\shell[] Queries value: HKCR\exefile\shell\open\command[] Queries value: HKCR\exefile\shell\open\command[command] HKCU\software\microsoft\windows\shellnoroam\muicache[c:\documents and Oueries value: settings\admin\application data\run32.exe] Queries value: HKCU\software\microsoft\visual basic\6.0[allowunsafeobjectpassing] HKLM\software\microsoft\windows nt\currentversion\compatibility32[run32] Oueries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[run32] HKLM\software\microsoft\internet Oueries value: explorer\main\featurecontrol\feature\_protocol\_lockdown[run32.exe] HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-Queries value: ab78-1084642581fb1 HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-Queries value: 0000-0000000000000 Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[appdata] HKCU\software\microsoft\windows\currentversion\run[cunt.exe] Oueries value: Queries value: HKLM\software\microsoft\windows\currentversion\run[cunt.exe] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[winsock\_registry\_version] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[serial\_access\_num] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[next\_catalog\_entry\_id] Queries value: Queries value:  $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries \ 000000000001 \ [packed catalog item]$ Oueries value: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000003[packedcatalogitem] Queries value: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000005[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000006[packedcatalogitem] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000007[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000008[packedcatalogitem] Oueries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000010[packedcatalogitem] Queries value: Queries value:  $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 [serial\_access\_num]$ Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[num\_catalog\_entries] Queries value:  $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace \_catalog5 \ catalog\_entries \ 00000000001 [library path]$ Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[displaystring] Queries 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] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[supportednamespace]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[storesserviceclassinfo]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[enabled]

Queries value:

Oueries value:

HKLM\system\currentcontrolset\services\winsockz\parameters\namespace\_catalogs\catalog\_entries\uuuuuuuuuuuul[storesserviceclassinto]
Queries value:

```
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ (catalog\_entries \ 000000000002[library path])
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap amespace\_catalog \\ S \setminus catalog\_entries \setminus 00000000000002[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
  Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000002[supported name space]
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus names pace\_catalog \\ \setminus catalog\_entries \setminus 00000000000002 [enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_entries\000000000002[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog S \setminus catalog\_entries \setminus 0000000000003[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[addressfamily]
  Queries value:
Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog 5 \setminus catalog\_entries \setminus 0000000000003 [enabled]
  Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ namespace\_catalog \ services \ namespace\_catalog \ namespace\_catal
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
  Queries value:
HKLM \verb| system| current control set \verb| services| dns cache \verb| parameters[used omain name devolution]|
HKLM\svstem\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [prioritize record data]
HKLM\svstem\currentcontrolset\services\dnscache\parameters[allowungualifiedguerv]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [screen badtlds]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
  Oueries value:
                                        \label{lem:hklm} \verb+kklm \system \current control set \services \dnscache \parameters [useedns]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
  Queries value:
                                        HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
  Oueries value:
```

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local_problem} \begin{tabular}{ll} HKLM \end{tabular} which is a parameter of the parameters of the paramet$ 

Queries value:

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [disable wandynamic update]$ 

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]  $\label{local-operator} \begin{tabular}{ll} HKLM\system\current controlset\services\dnscache\parameters[maxcachettl] \end{tabular}$ Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets] Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [multicast listen level]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel] HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts] Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [dnsmulticast query time outs]$ HKLM\system\currentcontrolset\services\tcpip\linkage[bind] Oueries value: c7d49d7cecdc}[enabledhcp] Queries value: c7d49d7cecdc}[leaseobtainedtime] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[leaseterminatestime] Oueries value: c7d49d7cecdc}[dhcpserver] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[queryadaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[disableadapterdomainname] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[registrationenabled] Oueries value: c7d49d7cecdc}[registeradaptername] Queries value: c7d49d7cecdc}[registrationmaxaddresscount] Oueries value: c7d49d7cecdc}[maxnumberofaddressestoregister] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[domain] Oueries value: c7d49d7cecdc}[dhcpdomain] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[ipautoconfigurationenabled] Oueries value:

```
c7d49d7cecdc}[addresstype]
 Oueries value:
c7d49d7cecdc}[nameserver]
 Oueries value:
c7d49d7cecdc}[dhcpnameserver]
                         HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
                         HKLM \verb|\software\microsoft\cryptography\defaults\provider\microsoft\ strong
 Oueries value:
cryptographic provider[type]
 Queries value:
                         HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
 Queries value:
                         HKLM\software\microsoft\cryptography[machineguid]
 Queries value:
                         HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
                         HKLM\system\currentcontrolset\services\winsock\parameters[transports]
 Oueries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [minsock addrlength]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
                         HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\run[skcjermegrebr]
 Queries value:
 Oueries value:
HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\calc.exe]
                         HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
 Oueries value:
77e8f3d1aa80}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}[dword]
                         HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
 Queries value:
77e8f3d1aa80}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}[dword]
 Oueries value:
                         HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}[dword]
                         HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
 Oueries value:
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[dword]
                         HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
 Queries value:
77e8f3d1aa80}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}[dword]
 Oueries value:
                         HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}[dword]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\aedebug[auto]
                         \label{lem:hklmsoftware} \verb+ MKLM \software \microsoft \windows nt \current version \aedebug [debugger]
 Oueries value:
                         HKLM\software\microsoft\pchealth\errorreporting[doreport]
 Oueries value:
 Queries value:
                         HKLM\software\microsoft\pchealth\errorreporting[showui]
 Oueries value:
                         HKLM\software\microsoft\pchealth\errorreporting[allornone]
 Queries value:
                         HKLM\software\microsoft\pchealth\errorreporting[includemicrosoftapps]
                         HKLM\software\microsoft\pchealth\errorreporting[includewindowsapps]
 Oueries value:
 Oueries value:
                         HKLM\software\microsoft\pchealth\errorreporting[dotextlog]
                         HKLM\software\microsoft\pchealth\errorreporting[includekernelfaults]
 Oueries value:
                         HKLM\software\microsoft\pchealth\errorreporting[includeshutdownerrs]
 Oueries value:
 Oueries value:
                         HKLM\software\microsoft\pchealth\errorreporting[numberoffaultpipes]
                         HKLM\software\microsoft\pchealth\errorreporting[numberofhangpipes]
 Queries value:
 Oueries value:
                         HKLM\software\microsoft\pchealth\errorreporting[maxuserqueuesize]
 Queries value:
                         HKLM\software\microsoft\pchealth\errorreporting[forcequeuemode]
 Oueries value:
HKLM\software\microsoft\pchealth\errorreporting\exclusionlist[explorer.exel
                         HKLM\software\microsoft\windows nt\currentversion\compatibility32[dwwin]
 Oueries value:
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[dwwin]
 Oueries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[dwwin.exe]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion[programfilesdir]
 Oueries value:
                         HKLM\software\microsoft\windows\currentversion[commonfilesdir]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion[digitalproductid]
 Queries value:
                         HKCU\software\microsoft\internet explorer\settings[anchor color]
 Oueries value:
                         HKLM\software\microsoft\pchealth\errorreporting\dw[buildpipemachine]
 Queries value:
                         HKLM\software\microsoft\pchealth\errorreporting\dw[dwfiletreeroot]
                         HKLM\software\microsoft\pchealth\errorreporting\dw[dwtracking]
 Queries value:
 Queries value:
                         HKLM\software\microsoft\pchealth\errorreporting\dw[dwnoexternalurl]
                         HKLM\software\microsoft\pchealth\errorreporting\dw[dwnofilecollection]
 Oueries value:
 Oueries value:
HKLM\software\microsoft\pchealth\errorreporting\dw[dwnosecondlevelcollection]
```

AKLM\software\microsoft\pcnealth\errorreporting\dw[dwnosecondlevelcollection]

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

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

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

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

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

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

settings[fromcachetimeout]

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

settings[secureprotocols]

```
Queries value:
                             HKLM\software\policies\microsoft\internet
explorer\main[security hklm only]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablekeepalive]
 Queries value:
                             \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
settings[disablepassport]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[cachemode]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[enablehttp1_1]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[proxyhttp1.1]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablenegotiate]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablebasicoverclearchannel]
                             HKCU\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
                             HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[clientauthbuiltinui]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[syncmode5]
                             HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[signature]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\content[peruseritem]
 Queries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\content[cacheprefix]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cachelimit]
 Queries value:
                             \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings\5.0\cache\cookies[peruseritem]
                             HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\cookies[peruseritem]
 Oueries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
 Queries value:
                             \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings\5.0\cache\cookies[cachelimit]
 Oueries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
                             \label{lem:hklm} \verb+Kklm\+ software\+ incressft\+ windows\+ current version\+ internet
 Oueries value:
settings\5.0\cache\history[peruseritem]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\history[cacheprefix]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
 Oueries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacherepair]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cachepath]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheprefix]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cacheoptions]
 Queries value:
                             \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\extensible cache\feedplat[cacherepair]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
 Queries value:
                             \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\extensible cache\feedplat[cachelimit]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacherepair]
 Queries value:
                             \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\extensible cache\iecompat[cachepath]
```

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

Queries value:

```
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cachelimit]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
 Queries value:
settings\5.0\cache\extensible cache\ietld[cacherepair]
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
 Oueries value:
settings\5.0\cache\extensible cache\ietld[cachepath]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
 Queries value:
settings\5.0\cache\extensible cache\ietld[cachelimit]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
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]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[socketsendbufferlength]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[socketreceivebufferlength]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxhttpredirects]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsper1_0server]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsper1_0server]
 Queries value:
                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[maxconnectionsperproxy]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[serverinfotimeout]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connectretries]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[connectretries]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
 Oueries 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]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablentlmpreauth]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[scavengecachelowerbound]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelifetime]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[httpdefaultexpirytimesecs]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[ftpdefaultexpirytimesecs]
                           HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[dwwin.exe]
 Oueries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablecachingofsslpages]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[perusercookies]
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Oueries value:
settings[leashlegacycookies]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablent4rascheck]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dialupuselansettings]
 Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendextracrlf]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypassftptimecheck]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduringauth]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[releasesocketduring401auth]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[releasesocketduring401auth]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
 Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasshttpnocachecheck]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[enablehttptrace]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[nocheckautodialoverride]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dontusednsloadbalancing]
 Queries value:
                           \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
settings[dontusednsloadbalancing]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[mimeexclusionlistforcache]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[headerexclusionlistforcache]
 Queries value:
                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[dnscacheenabled]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dnscacheentries]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[dnscachetimeout]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
```

```
settings[warnonpost]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnalwaysonpost]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
  Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
settings[warnonbadcertsending]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonbadcertrecving]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
  Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[alwaysdrainonredirect]
                           \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{$microsoft$} \windows \current version \end{tabular} \label{thm:local_hammon_hammon} \end{tabular}
 Queries value:
settings[warnonhttpstohttpredirect]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
                           HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[urlencoding]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[truncatefilename]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[badproxyexpirestime]
  Queries value:
Queries value:
HKLM\software\microsoft\tracing[enableconsoletracing]
  Queries value:
                           HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
  Oueries value:
                           HKLM \setminus software \setminus microsoft \setminus tracing \setminus rasapi 32 [filetracing mask]
  Queries value:
                           HKLM \setminus software \setminus microsoft \setminus tracing \setminus rasapi32 [enable consoletracing]
  Queries value:
  Queries value:
                           HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
  Oueries value:
                           HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
                           HKLM\software\microsoft\tracing\rasapi32[filedirectory]
  Queries value:
                           HKLM\software\microsoft\windows\currentversion\explorer\user shell
  Oueries value:
folders[common appdata]
                           HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\profilelist[profilesdirectory]
  Queries value:
                           HKLM\software\microsoft\windows
nt\currentversion\profilelist[allusersprofile]
                           HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\profilelist[defaultuserprofile]
                           HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
  Oueries value:
1757981266-507921405-1957994488-1003[profileimagepath]
  Oueries value:
                           HKCU\software\microsoft\windows
nt\currentversion\winlogon[parseautoexec]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[migrateproxy]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[proxyenable]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[proxyoverride]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
                           \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
  Queries value:
settings\connections[savedlegacysettings]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
                           HKCU\software\microsoft\windows nt\currentversion\windows[scrollinset]
  Queries value:
                           HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
  Oueries value:
  Queries value:
                           HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]
                           HKCU\software\microsoft\windows nt\currentversion\windows[scrolldelay]
  Oueries value:
  Queries value:
                           HKCU\software\microsoft\windows
nt\currentversion\windows[scrollinterval]
  Queries value:
                           HKLM\software\microsoft\rpc\securityservice[10]
  Oueries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
                           HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
  Oueries value:
  Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]
  Queries value:
                           HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]
  Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[version]
  Oueries value:
                           HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]
  Queries value:
                           HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]
```

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

Oueries value:

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

HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version] Oueries value: Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]

Oueries value:

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

 $HKLM \setminus system \setminus current control \setminus lsa \setminus sspicache \setminus msnsspc.dll[name]$ Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment] Queries value:

Oueries value:

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

Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid] HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version] Oueries value: Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type]

Queries value:

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

Queries value: HKCU\appevents\schemes\apps\.default\systemnotification\.current[]

Sets/Creates value:

 $HKCU \ software \ microsoft \ windows \ shell no roam \ muicache \ [c:\docume-1\admin\locals-1\temp\cpegx.bat]$ 

Sets/Creates value: HKCU\software\microsoft\windows\currentversion\run[run32.dll]

Sets/Creates value: HKCU\software\microsoft\windows\shellnoroam\muicache[c:\documents and

settings\admin\application data\run32.exel

Sets/Creates value: HKCU\software\microsoft\windows\currentversion\run[cunt.exe] Sets/Creates value: HKLM\software\microsoft\windows\currentversion\run[cunt.exe] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\run[skcjermegrebr]

Sets/Creates value:

HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\calc.exe]

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

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

folders[personal] Value changes:

806d6172696f}[baseclass]

 $\label{lem:hklm} \verb+Kklm\+ software\+ windows\+ current version\+ explorer\+ shell$ Value changes:

folders[common documents]

Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[desktop] Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell

folders[common desktop]

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

settings\zonemap[proxybypass]

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

settings\zonemap[intranetname]

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

settings\zonemap[uncasintranet]

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

settings\zonemap[autodetect] Value changes:

HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cache]

Value changes:

HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cookies]

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

Value changes: folders[appdata]

HKCU\sessioninformation[programcount] Value changes:

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

folders[history]

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

folders[common appdata]

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

settings[proxyenable]

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

settings\connections[savedlegacysettings]