Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3309, Task ID: 744

Task ID: 744 Risk Level: 10

Date Processed: 2016-05-18 10:33:01 (UTC)

Processing Time: 61.58 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\6b0dfa86acf4bfbdf5c34927f9b3e733.exe"

Sample ID: Type: basic admin Owner:

6b0dfa86acf4bfbdf5c34927f9b3e733 Label: 2016-05-18 10:30:48 (UTC) Date Added:

PE32:win32:gui File Type:

File Size: 155648 bytes

6b0dfa86acf4bfbdf5c34927f9b3e733 MD5:

2a5e99090310812a6d7d02c07e70d3fc29d3588998de27d4f54e4a5f73a017f3 SHA256:

Description: None

Pattern Matching Results

Modifies registry autorun entries

10 Creates malicious events: Vobfus [Worm]

5 Adds autostart object

5 Creates process in suspicious location

Process/Thread Events

C:\WINDOWS\Temp\6b0dfa86acf4bfbdf5c34927f9b3e733.exe Creates process:

["c:\windows\temp\6b0dfa86acf4bfbdf5c34927f9b3e733.exe"]

Creates process: C:\WINDOWS\Temp\6b0dfa86acf4bfbdf5c34927f9b3e733.exe [71] C:\Documents and Settings\Admin\boauh.exe ["C:\Documents and Creates process:

Settings\Admin\boauh.exe"]

Creates process: C:\Documents and Settings\Admin\boauh.exe [71]

Writes to process: PID:1884 C:\WINDOWS\Temp\6b0dfa86acf4bfbdf5c34927f9b3e733.exe

Writes to process: PID:504 C:\Documents and Settings\Admin\boauh.exe C:\WINDOWS\Temp\6b0dfa86acf4bfbdf5c34927f9b3e733.exe Terminates process:

C:\Documents and Settings\Admin\boauh.exe Terminates process:

Named Object Events

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

1957994488-1003 Creates mutex:

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

1957994488-1003 Creates mutex:

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

1957994488-1003

\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\A Creates mutex:

\BaseNamedObjects\ZonesCounterMutex Creates mutex:

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

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

\BaseNamedObjects\C:?WINDOWS?TEMP?6B0DFA86ACF4BFBDF5C34927F9B3E733.EXE Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1} Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D} Creates semaphore: Creates semaphore: \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57} Creates semaphore: \BaseNamedObjects\C:?DOCUMENTS AND SETTINGS?ADMIN?BOAUH.EXE

File System Events

Creates C:\Documents and Settings\Admin\boauh.exe

C:\Documents and Settings\Admin Opens: 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 C:\WINDOWS\system32\MSCTFIME.IME Opens: Opens: C:\WINDOWS\system32\clbcatq.dll C:\WINDOWS\system32\comres.dll Opens:

C:\WINDOWS\Registration\R00000000007.clb Opens:

Opens: C:\WINDOWS\Temp\6b0dfa86acf4bfbdf5c34927f9b3e733.exe

Opens: C:\WINDOWS\system32\apphelp.dll

```
C:\WINDOWS\AppPatch\sysmain.sdb
 Opens:
 Opens:
                         C:\WINDOWS\AppPatch\systest.sdb
 Opens:
                         C:\WINDOWS\Temp
 Opens:
 Opens:
                         C:\WINDOWS
 Opens:
                         C:\windows\temp\6b0dfa86acf4bfbdf5c34927f9b3e733.exe.Manifest
 Opens:
                         C:\WINDOWS\Prefetch\6B0DFA86ACF4BFBDF5C34927F9B3E-0FAA7DB6.pf
                         C:\WINDOWS\WINHELP.INI
 Opens:
                         C:\WINDOWS\system32\shell32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\shell32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\shell32.dll.124.Config
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
 Opens:
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
 Opens:
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
                         C:\WINDOWS\WindowsShell.Manifest
 Opens:
                         C:\WINDOWS\WindowsShell.Config
 Opens:
                         C:\WINDOWS\system32\comctl32.dll
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Manifest
                         C:\WINDOWS\system32\comctl32.dll.124.Config
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\boauh.exe
 Opens:
                         C:\WINDOWS\system32\netapi32.dll
 Opens:
                         C:\WINDOWS\system32\setupapi.dll
 Opens:
                         C:\Documents and Settings
 Opens:
                         C:\Documents and Settings\Admin\My Documents\desktop.ini
                         C:\Documents and Settings\All Users
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Documents\desktop.ini
 Opens:
                         C:\WINDOWS\system32\urlmon.dll
                         C:\WINDOWS\system32\urlmon.dll.123.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Config
 Opens:
                         C:\Documents and Settings\Admin\boauh.exe.Manifest
```

C:\WINDOWS\Prefetch\BOAUH.EXE-053BB084.pf Opens:

Opens: C:\WINDOWS\system32\ws2_32.dll C:\WINDOWS\system32\ws2help.dll Opens: C:\WINDOWS\system32\mswsock.dll Opens: Opens: C:\WINDOWS\system32\hnetcfg.dll Opens: C:\WINDOWS\system32\wshtcpip.dll

Opens: C:\WINDOWS\system32\dnsapi.dll Opens: C:\WINDOWS\system32\iphlpapi.dll Opens: C:\WINDOWS\system32\winrnr.dll Opens: C:\WINDOWS\system32\drivers\etc\hosts Opens: C:\WINDOWS\system32\rsaenh.dll Opens: C:\WINDOWS\system32\crypt32.dll C:\WINDOWS\system32\rasadhlp.dll Opens: Opens: C:\WINDOWS\system32\MSIMTF.dll

Writes to: C:\Documents and Settings\Admin\boauh.exe Reads from: C:\WINDOWS\Registration\R00000000007.clb

Reads from: $C: \verb|\WINDOWS\Temp\6b0dfa86acf4bfbdf5c34927f9b3e733.exe|\\$ Reads from: C:\Documents and Settings\Admin\My Documents\desktop.ini Reads from: C:\Documents and Settings\All Users\Documents\desktop.ini

Reads from: C:\Documents and Settings\Admin\boauh.exe Reads from: C:\WINDOWS\system32\drivers\etc\hosts Reads from: C:\WINDOWS\system32\rsaenh.dll

Network Events

DNS query:	ns1.boxonline1.com
DNS query:	ns1.boxonline1.net
DNS query:	ns1.boxonline1.org
DNS query:	ns1.boxonline2.com
DNS query:	ns1.boxonline2.net
DNS query:	ns1.boxonline2.org
DNS query:	ns1.boxonline3.com
DNS query:	ns1.boxonline3.net
DNS query:	ns1.boxonline3.org
Sends data to:	8.8.8.8:53
Receives data from:	0.0.0.0:0

Windows Registry Events

	0 3
Creates key:	HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders	
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\explorer\shell folders</pre>
Creates key:	
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-	
806d6172696f}\	
Creates key:	<pre>HKLM\software\microsoft\windows\currentversion\explorer\user shell</pre>
folders	
Creates key:	<pre>HKLM\software\microsoft\windows\currentversion\explorer\shell folders</pre>
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\run\</pre>
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\explorer\advanced\</pre>

Creates key: $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus windows \cup policies \setminus microsoft \setminus windows \cup policies \setminus microsoft \setminus windows \cup policies \setminus microsoft \cup policies \setminus microsoft \cup policies \cup polic$ Creates key: HKLM\software

Creates key: HKLM\software\policies Creates key: HKLM\software\policies\microsoft

Creates key: HKLM\software\policies\microsoft\windows

Creates key: HKLM\software\policies\microsoft\windows\windowsupdate Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters

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

options\6b0dfa86acf4bfbdf5c34927f9b3e733.exe

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

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

options\gdi32.dll

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

options\user32.dll

Opens key: HKLM\system\currentcontrol\session manager

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

options\imm32.dll

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

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

options\advapi32.dll

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

options\msvcrt.dll

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

options\ole32.dll

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

options\oleaut32.dll

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
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility

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

Opens key: HKLM\

 $Opens\;key: \\ \qquad \qquad \text{HKLM} software \\ \text{microsoft} \\ \text{windows}\;\; nt \\ \text{current} \\ \text{version} \\ \text{diagnostics}$

Opens key: HKLM\software\microsoft\ole

Opens key: HKCR\interface

Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}

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:

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

options\msctfime.ime

Opens key: HKCU\software\microsoft\ctf

Opens key: ${\tt HKLM \setminus software \setminus microsoft \setminus ctf \setminus systems hared}$

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

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

Opens key: HKLM\software\microsoft\com3

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

options\comres.dll

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

options\clbcatq.dll

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

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

Opens key: HKU\
Opens key: HKCR\clsid

Opens key: HKCU\software\classes\clsid\{a4341dcc-5064-42df-9638-3b4a33c14bd4}

Opens key: HKCR\clsid\{a4341dcc-5064-42df-9638-3b4a33c14bd4}

Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\apphelp.dll

Opens key: HKLM\system\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\6b0dfa86acf4bfbdf5c34927f9b3e733.exe

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

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

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-

be2efd2c1a33}

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

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}

Opens key:

Opens key:

Opens key:

Opens kev:

Opens key:

 $HKLM \verb|\software\policies\microsoft\windows\safer\codeidentifiers\olines$

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths

Opens key:

 $\label{lem:hklm} HKLM \software \policies \microsoft \windows \safer \code identifiers \allow \allows \allow$

Opens key:

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

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

 $Opens \ key: \\ HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 65536 \ verlzones \\$

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

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

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

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

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

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

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

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

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

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

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

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

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

 $\label{two-policies} HKCU\software \policies \microsoft\windows \safer\code identifiers \code identi$

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

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

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

 $\label{lem:hkculsoftware} HKCU \software \policies \microsoft \windows \safer \code identifiers \cod$

Opens key:

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

 $\label{thm:local_explorer} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \shell folders \end{tabular}$ Opens key:

HKLM\software\microsoft\windows Opens key:

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

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

options\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

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

options\comctl32.dll

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

options\userenv.dll

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

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

folders

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

1757981266-507921405-1957994488-1003

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

Opens key:

 $HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ applications \ 6b0dfa86acf4bfbdf5c34927f9b3e733. execute \ microsoft \ microsoft$

Opens kev: 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

Opens key: ${\it HKLM} \verb|\software\microsoft\pc\pagedbuffers|$

Opens key: HKLM\software\microsoft\rpc

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

options\6b0dfa86acf4bfbdf5c34927f9b3e733.exe\rpcthreadpoolthrottle Opens key: HKLM\software\policies\microsoft\windows nt\rpc HKLM\system\currentcontrolset\control\computername Opens key:

Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer Opens key: $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ policies\+ explorer$ Opens key:

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

a2d8-08002b30309d}

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

08002b30309d}\inprocserver32

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

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

HKCR\drive\shellex\folderextensions Opens kev:

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

4442-804e-409d6c4515e9}

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

409d6c4515e9}

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

HKCU\software\classes\.exe Opens key:

Opens key: HKCR\.exe

Opens key: HKCU\software\classes\exefile

HKCR\exefile Opens key:

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

Opens key: HKCR\exefile\curver

Opens key: HKCR\exefile\

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

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

Opens key: HKCR\exefile\shellex\iconhandler

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

Opens key: HKCR\systemfileassociations\.exe

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

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

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

HKCR* Opens key:

Opens key: HKCU\software\classes*\clsid

Opens kev: HKCR*\clsid

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

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

11e3-9fc7-806d6172696f}\

HKCU\software\classes\directory Opens key:

Opens key: HKCR\directory

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

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

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

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

Opens key: HKCR\directory\clsid

HKCU\software\classes\folder Opens kev:

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

00c04fd91972}\inprocserver32

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

HKCU\software\classes\.app Opens key:

Opens key: HKCR\.app

Opens key: HKCU\software\classes\.asp

HKCR\.asp Opens key:

Opens key: HKCU\software\classes\.bas

Opens key: HKCR\.bas

HKCU\software\classes\.bat Opens key:

Opens key: HKCR\.bat Opens key:

HKCU\software\classes\.cer

Opens key: HKCR\.cer

Opens key: HKCU\software\classes\.chm

Opens key: HKCR\.chm

HKCU\software\classes\.cmd Opens key:

Opens key: HKCR\.cmd

Opens key: HKCU\software\classes\.com

Opens key: HKCR\.com

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

Opens key:

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

Opens key: HKCR\.csh

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

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

00c04fb6bfc4}\treatas

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

00c04fb6bfc4}\inprocserver32

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

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

00c04fb6bfc4}\inprocserverx86

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

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

00c04fb6bfc4}\localserver32

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

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

00c04fb6bfc4}\inprochandler32

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

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

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

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\

HKCR\protocols\name-space handler Opens kev:

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
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
                                      HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_protocol_lockdown
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\
  Opens key:
                                      \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ internet\ explorer\+ main\+ feature control
  Opens key:
                                      HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
                                      \label{lem:hammon} \mbox{HKLM\software\mbox{\sc microsoft\internet explorer\mbox{\sc main\sc main\sc
  Opens key:
  Opens key:
                                      HKCU\software\microsoft\internet explorer\main\featurecontrol
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
  Opens key:
                                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
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 key:
settings\zonemap\ranges\
                                      HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:
                                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\zonemap\
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
                                      HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
  Opens key:
                                      HKLM\software\policies
  Opens key:
                                      HKCU\software\policies
  Opens key:
                                      HKCU\software
  Opens key:
                                      HKI M\software
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\protocoldefaults\
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\zonemap\domains\
  Opens key:
                                      HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:
                                      HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\msn.com
                                      HKLM\software\microsoft\windows\currentversion\internet
  Opens 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
  Opens key:
                                      HKCU\software\microsoft\internet explorer\ietld
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610
  Opens key:
                                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610
                                      HKCU\software\microsoft\windows\currentversion\internet settings
  Opens key:
  Opens kev:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
                                      HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_http_username_password_disable
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
  Opens kev:
                                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
  Opens kev:
                                      HKLM\software\policies\microsoft\internet explorer
```

Opens key: HKLM\software\policies\microsoft\internet explorer\security

Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\ Opens key: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\sl}} \mbox{\tt zones\sl} \mbox{\tt 0}$ Opens kev: 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 HKCU\software\microsoft\windows\currentversion\internet settings\zones\4 Opens kev:

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

settings\zones\

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

settings\zones\

```
Opens key:
                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
   Opens key:
                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\1
  Opens key:
                                                  HKCU\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 key:
settings\zones\2
  Opens key:
                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
   Opens key:
                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
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
                                                  HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
                                                  HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_localmachine_lockdown
  Opens key:
                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\
                                                  HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\
                                                  HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\0
                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\0
                                                  \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} internet \end{tabular}
   Opens key:
settings\lockdown_zones\0
                                                  HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\1
                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\1
                                                  \label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu} \mbox{\tt hkcu\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\color=lem:hkcu\soft\windows\currentversion\color=lem:hkcu\soft\windows\currentversion\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu
   Opens key:
settings\lockdown_zones\1
                                                  HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\2
                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\2
   Opens key:
                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
                                                  HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\3
   Opens key:
                                                  \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\3
   Opens key:
                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                                                  HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\4
   Opens key:
                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\4
  Opens key:
                                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
                                                  HKLM\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature zones default drive intranet kb941000
   Opens key:
                                                  HKCU\software\classes\exefile\shell
   Opens kev:
                                                  HKCR\exefile\shell
   Opens key:
                                                  HKCU\software\classes\exefile\shell\open
   Opens key:
                                                  HKCR\exefile\shell\open
   Opens key:
                                                  HKCU\software\classes\exefile\shell\open\command
   Opens kev:
                                                  HKCR\exefile\shell\open\command
   Opens key:
HKCU\software\microsoft\windows\currentversion\policies\explorer\restrictrun
                                                  HKLM\software\microsoft\windows\currentversion\app paths\boauh.exe
   Opens kev:
   Opens key:
                                                  HKCU\software\classes\exefile\shell\open\ddeexec
   Opens key:
                                                  HKCR\exefile\shell\open\ddeexec
   Opens key:
                                                  HKCU\software\classes\applications\boauh.exe
   Opens key:
                                                  HKCR\applications\boauh.exe
                                                  HKCU\software\microsoft\windows\shellnoroam
   Opens key:
   Opens key:
                                                  HKCU\software\microsoft\windows\shellnoroam\muicache
   Opens key:
                                                  HKCU\software\microsoft\windows\shellnoroam\muicache\
   Opens key:
                                                  HKLM \verb|\software\m| icrosoft \verb|\windows\currentversion\explorer\file association | in the constant of the co
   Opens key:
                                                  HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\boauh.exe
```

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

options\boauh.exe

Opens key: HKLM\software\microsoft\ctf\compatibility\boauh.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\system\currentcontrolset\services\winsock2\parameters Opens key:

Opens key:

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

Opens kev:

Opens key:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000 Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007 Opens kev:

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010 Opens kev:

Opens kev:

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

Opens key:

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

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

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000003

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

options\mswsock.dll

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

options\hnetcfg.dll

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

Opens key: $\label{lem:hklm} \verb+Kklm \system \current control set \services \swinsock \space{2mm} parameters$ Opens kev: HKLM\svstem\currentcontrolset\services\tcpip\parameters\winsock Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\wshtcpip.dll

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

options\dnsapi.dll

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

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

options\iphlpapi.dll

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

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

 ${\tt HKLM \backslash system \backslash current control set \backslash services \backslash net bt \backslash parameters}$ Opens key:

Opens key:

c7d49d7cecdc}

Opens key:

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

options\wldap32.dll

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

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

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

Opens key: HKLM\software\microsoft\cryptography

Opens kev: ${\tt HKLM \ } software \ \verb|\ microsoft \ \verb|\ cryptography \ \verb|\ offload|$ Opens key: HKLM\system\currentcontrolset\control\wmi\security Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\rasadhlp.dll

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

Queries value:

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

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

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

nt\currentversion\compatibility32[6b0dfa86acf4bfbdf5c34927f9b3e733]

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

compatibility[6b0dfa86acf4bfbdf5c34927f9b3e733]

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

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

manager[criticalsectiontimeout]

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

Queries value: HKCR\interface[interfacehelperdisableall]

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

000000000046}[interfacehelperdisableall]

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

00000000046}[interfacehelperdisableallforole32]

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

manager[safeprocesssearchmode]

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

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

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

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

Queries value: HKLM\software\microsoft\com3[regdbversion]
Queries value: HKLM\system\currentcontrol\session

manager\appcompatibility[disableappcompat]

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

Queries value:

 $HKLM \ "software \ "policies \ "microsoft \ "windows \ "safer \ "code identifiers \ [authenticode enabled]$

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

Queries value:

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[itemdata]

Queries value:

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[itemsize]

Queries value:

Queries value:

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

Queries value:

 $\label{thm:hklm} HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}\ [hashalg]$

Queries value:

HKLMNsoftware\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91\Fitemsize\

Queries value:

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

Queries value:

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

Queries value:

```
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{81d1fe15-dd9d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16
7c29ddecae3f}[hashalg]
        Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemsize]
        Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[saferflags]
        Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemdata]
        Queries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus soften \setminus code identifiers \setminus 0 \setminus hashes \setminus \{94e3e076-8f53-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-42a5-8411-426-8411-426-8411-426-8411-
085bcc18a68d}[hashalg]
        Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemsize]
        Queries value:
085bcc18a68d}[saferflags]
        Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemdata]
```

b91490411bfc}[hashalg]

Queries value:

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

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

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

Oueries value:

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

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

folders[cache]

Queries value:

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

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

Oueries value:

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\winlogon[userenvdebuglevel]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\winlogon[chkaccdebuglevel]

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

folders[local settings]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\winlogon[rsopdebuglevel]

Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging] HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-Oueries value:

1757981266-507921405-1957994488-1003[profileimagepath]

Oueries value: HKLM\system\currentcontrolset\services\disk\enum[0]

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

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

Queries value:

HKLM\svstem\currentcontrolset\computername\activecomputername[computername] Queries value:

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

 $HKCU \ software \ microsoft \ windows \ current version \ policies \ \ explorer [no properties my computer]$ Queries value:

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

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

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

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

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

409d6c4515e9}[drivemask]

Oueries value:

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

HKCR\.exe[] Oueries value:

Queries value:

```
HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
                                                HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
   Oueries value:
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[forceactivedesktopon]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
                                                HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
   Oueries value:
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
   Queries value:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{lem:hkcu} advanced \cite{lem:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
   Queries value:
                                                HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
   Queries value:
\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{tabular} is a constant \cite{tabular} and \cite{tabular} is a constant \cite{tabular} and \cite{tabular} is a constant \cite{tabular} is a constant \cite{tabular} and \
   Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced [separate process]
   Oueries value:
HKCR\exefile[docobject]
   Queries value:
                                                HKCR\exefile[browseinplace]
   Queries value:
   Oueries value:
                                                HKCR\exefile[isshortcut]
                                                 HKCR\exefile[alwaysshowext]
   Queries value:
   Oueries value:
                                                 HKCR\exefile[nevershowext]
   Oueries value:
                                                HKLM\system\wpa\pnp[seed]
                                                 HKLM\system\setup[osloaderpath]
   Oueries value:
   Queries value:
                                                 HKLM\system\setup[systempartition]
   Queries value:
                                                HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus setup[sourcepath]
   Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
   Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]
                                                HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
   Oueries value:
   Queries value:
                                                HKLM\software\microsoft\windows\currentversion[devicepath]
   Queries value:
                                                 HKLM\software\microsoft\windows\currentversion\setup[loglevel]
   Oueries value:
                                                HKLM\software\microsoft\windows\currentversion\setup[logpath]
   Queries value:
                                                HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
   Oueries value:
                                                HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
   Oueries value:
11e3-9fc7-806d6172696f}[data]
   Queries value:
11e3-9fc7-806d6172696f}[generation]
   Oueries value:
                                                 HKCR\directorv[docobiect]
   Queries value:
                                                HKCR\directory[browseinplace]
                                                 HKCR\directory[isshortcut]
   Oueries value:
   Queries value:
                                                 HKCR\directory[alwaysshowext]
   Queries value:
                                                HKCR\directory[nevershowext]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[comparejunctionness]
                                                HKLM\software\microsoft\windows\currentversion\explorer\user shell
   Oueries value:
folders[common documents]
   Queries value:
                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[desktop]
   Queries value:
                                                 HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common desktop]
                                                 HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32[]
   Oueries value:
   Oueries value:
                                                HKCR\clsid\{aeb6717e-7e19-11d0-97ee-
00c04fd91972}\inprocserver32[loadwithoutcom]
                                                HKCR\.asp[]
   Oueries value:
   Queries value:
                                                 HKCR\.bat[]
```

```
Oueries value:
                                                   HKCR\.cer[]
                                                   HKCR\.chm[]
   Oueries value:
   Oueries value:
                                                   HKCR\.cmd[]
   Queries value:
                                                   HKCR\.com[]
                                                   HKCR\.cplf1
   Oueries value:
   Queries value:
                                                   HKCR\.crt[]
   Oueries value:
                                                   HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[inprocserver32]
   Queries value:
                                                   HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[]
                                                   HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[appid]
   Oueries value:
                                                   HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
   Oueries value:
00c04fb6bfc4}\inprocserver32[threadingmodel]
                                                   HKLM\software\microsoft\windows\currentversion\internet
   Queries value:
settings[disableimprovedzonecheck]
                                                   HKLM\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_protocol_lockdown[6b0dfa86acf4bfbdf5c34927f9b3e733.exe]
   Queries value:
                                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
   Queries value:
                                                   HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
                                                   HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
   Oueries value:
   Queries value:
                                                   HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
                                                   \label{lem:hklm} \verb+ HKLM \+ software \+ microsoft \+ windows \+ current version \+ internet
   Oueries value:
settings[createuricachesize]
                                                   HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[enablepunycode]
                                                   HKLM\software\microsoft\windows\currentversion\internet
   Queries value:
settings[enablepunycode]
                                                   HKLM\software\policies\microsoft\internet
   Oueries value:
explorer\security[disablesecuritysettingscheck]
                                                   HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\zones\0[flags]
                                                   HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\zones\1[flags]
   Queries value:
                                                   HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[flags]
                                                   HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\zones\3[flags]
                                                   HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\zones\4[flags]
                                                   HKCU\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[6b0dfa86acf4bfbdf5c34927f9b3e733.exe]
                                                   HKCU\software\microsoft\internet
   Oueries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
   Oueries value:
                                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[6b0dfa86acf4bfbdf5c34927f9b3e733.exe]
   Queries value:
                                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
   Oueries value:
                                                   HKCU\software\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
   Oueries value:
                                                   HKLM\software\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
   Queries value:
                                                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
   Oueries value:
                                                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
   Oueries value:
                                                   HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1806]
   Queries value:
                                                   HKCR\exefile\shell[]
                                                   HKCR\exefile\shell\open\command[]
   Queries value:
   Queries value:
                                                   HKCR\exefile\shell\open\command[command]
   Queries value:
                                                   \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \software \verb|\microsoft| windows nt \current version \profile list \s-1-5-21-1000 \end{tabular} .
1757981266-507921405-1957994488-1003[flags]
   Oueries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[state]
                                                   \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} in the current version \end{tabular} profile list \end{tabular} is the current version \end{tabular} and the current version \
   Oueries value:
1757981266-507921405-1957994488-1003[userpreference]
                                                   HKLM \  \  \, nt\  \  \, in\  \  \, nt\  \  \, in\  \  \, i
   Queries value:
1757981266-507921405-1957994488-1003[centralprofile]
                                                   HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
   Oueries value:
1757981266-507921405-1957994488-1003[profileloadtimelow]
   Oueries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[profileloadtimehigh]
   Queries value:
                                                   HKCU\software\microsoft\windows\shellnoroam\muicache[langid]
   Queries value:
                                                   \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \shell no roam \muicache \cite{tabular} e. \label{linear} \end{tabular}
settings\admin\boauh.exel
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\fileassociation[cutlist]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[inheritconsolehandles]
HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun]
   Queries value:
```

HKCU\software\microsoft\windows\currentversion\policies\explorer[disallowrun] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[norunasinstallprompt] Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[boauh] HKLM\software\microsoft\windows nt\currentversion\ime Oueries value: compatibility[boauh] Oueries 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: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem] Oueries value: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ catalog_entries \ 00000000000003 \ [packed catalog item]$ Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000005[packedcatalogitem] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem] 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: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000009[packedcatalogitem] HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\00000000010[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num] HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5[num catalog entries] Oueries value: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace _catalog5 \ catalog_entries \ 00000000001 [library path]$ Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled] Queries value: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000002[librarypath] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog 5 \setminus catalog_entries \setminus 00000000000002[displaystring]$ Queries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily] Queries value: Queries value: Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog 5 \setminus catalog_entries \setminus 00000000000002 [version]$ Queries value: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog5 \ catalog_entries \ 10000000000002 \ [storesservice classinfo]$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[displaystring]

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

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000003 [supported name space]]$

Queries value:

Queries value:

Oueries value:

Queries value:

Queries value:

```
Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap services \setminus mame space\_catalog \\ \setminus catalog\_entries \setminus 00000000000003 [version]
  Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog\_entries \ (00000000003[storesserviceclass info]) \ (catalog\_entries) \ 
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
  Queries value:
                                    HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
                                    HKLM\svstem\currentcontrolset\services\winsock\parameters[transports]
  Oueries value:
  Queries value:
                                    HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  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]
  Queries value:
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| tcpip| parameters [usedomain named evolution]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
  Queries value:
                                    HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
  Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[guervipmatching]
  Queries value:
                                    HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
  Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [update top level domain zones]
  Queries value:
                                HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
  Oueries value:
                                 HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
                                {\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ dns cache \verb|\ parameters [max cachettl]|
  Oueries value:
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
  Queries value:
  Queries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-a
c7d49d7cecdc}[enabledhcp]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[leaseobtainedtime]
  Queries value:
c7d49d7cecdc}[leaseterminatestime]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpserver]
  Queries value:
c7d49d7cecdc}[queryadaptername]
  Oueries value:
c7d49d7cecdc}[disableadapterdomainname]
  Queries value:
c7d49d7cecdc}[registrationenabled]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registeradaptername]
  Oueries value:
c7d49d7cecdc}[registrationmaxaddresscount]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[maxnumberofaddressestoregister]
  Oueries value:
c7d49d7cecdc}[domain]
  Queries value:
c7d49d7cecdc}[dhcpdomain]
  Oueries value:
c7d49d7cecdc}[ipautoconfigurationenabled]
  Queries value:
c7d49d7cecdc}[addresstype]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[nameserver]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpnameserver]
  Oueries value:
                                HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
                                HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
  Oueries value:
  Oueries value:
                                HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
                                HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} wicrosoft \ strong
  Oueries value:
cryptographic provider[image path]
```

HKLM\software\microsoft\cryptography[machineguid] Queries value:

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

ab78-1084642581fb]

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

0000-000000000000000

Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]

HKLM\software\microsoft\windows\currentversion[programfilesdir] Queries value: HKCU\software\microsoft\windows\shellnoroam\muicache[c:\documents and Sets/Creates value:

settings\admin\boauh.exe]

HKCU\software\microsoft\windows\currentversion\run[boauh] Sets/Creates value:

Sets/Creates value:

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

Sets/Creates value: HKLM\software\policies\microsoft\windows\windowsupdate\au[noautoupdate]

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

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

folders[personal] Value changes:

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

806d6172696f}[baseclass]

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

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

settings\zonemap[proxybypass]

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

settings\zonemap[intranetname]

Value changes:

HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap[uncasintranet]

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

Value changes:

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

HKLM\software\policies\microsoft\windows\windowsupdate\au[noautoupdate] Value changes:

HKCU\software\microsoft\windows\currentversion\run[boauh]