Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3307, Task ID: 736

Task ID: 736 Risk Level: 10

Date Processed: 2016-05-18 10:31:50 (UTC)

Processing Time: 61.38 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\6b78f38317a53920e530cc1e36053242.exe"

Sample ID: Type: basic Owner: admin

6b78f38317a53920e530cc1e36053242 Label:

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

PE32:win32:gui File Type: File Size: 407933 bytes

6b78f38317a53920e530cc1e36053242 MD5:

cd43eae17643cd5510d87ca5b49ddb5b45f73b83c169dcd1102b356633943046 SHA256:

Description: None

Pattern Matching Results

Writes to memory of system processes

2 PE: Nonstandard section

7 Injects thread into Windows process

Possible kernel API resolver

Attempts to connect to dynamic DNS

4 Reads process memory

5 PE: Contains compressed section

Creates ActiveSetup run key

Packer: PECompact

10 Creates malicious mutex: Bifrost [APT, RAT, MoreInfo]

Static Events

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

Packer:

Process/Thread Events

C:\WINDOWS\Temp\6b78f38317a53920e530cc1e36053242.exe Creates process:

["c:\windows\temp\6b78f38317a53920e530cc1e36053242.exe"]

C:\WINDOWS\Temp\6b78f38317a53920e530cc1e36053242.exe Creates process:

[c:\windows\temp\6b78f38317a53920e530cc1e36053242.exe]

C:\Program Files\Internet Explorer\iexplore.exe ["C:\Program Creates process:

Files\Internet Explorer\IEXPLORE.EXE"]

PID:1488 C:\WINDOWS\Temp\6b78f38317a53920e530cc1e36053242.exe Reads from process: Reads from process: PID:512 C:\Program Files\Internet Explorer\iexplore.exe

Reads from process: PID:316 C:\WINDOWS\system32\calc.exe

Writes to process: PID:1488 C:\WINDOWS\Temp\6b78f38317a53920e530cc1e36053242.exe

PID:1992 C:\WINDOWS\explorer.exe Writes to process:

Writes to process: PID:512 C:\Program Files\Internet Explorer\iexplore.exe C:\WINDOWS\Temp\6b78f38317a53920e530cc1e36053242.exe Terminates process:

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

Named Object Events

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

1957994488-1003

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

1957994488-1003

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

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\Bif1234 Creates mutex: Creates mutex: \BaseNamedObjects\Ook3s

\BaseNamedObjects\MSCTF.Shared.MUTEX.ANH Creates mutex:

Creates event:

 $\verb|\BaseNamedObjects\CTF.ThreadMarshalInterfaceEvent.000000E0.00000000.00000004| \\$

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

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

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

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

File System Events

```
Creates
                         C:\Program Files\Bifrost
 Creates
                         C:\Program Files\Bifrost\server.exe
 Opens:
                         C:\WINDOWS\Prefetch\6B78F38317A53920E530CC1E36053-0977A58F.pf
 Opens:
                         C:\Documents and Settings\Admin
                         C:\WINDOWS\system32\winmm.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\imm32.dll
 Opens:
                         C:\WINDOWS\system32\comctl32.dll
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Config
                         C:\WINDOWS\system32\MSCTF.dll
 Opens:
                         {\tt C:\WINDOWS\system32\MSCTFIME.IME}
 Opens:
 Opens:
                         C:\WINDOWS\Temp\6b78f38317a53920e530cc1e36053242.exe
 Opens:
                         C:\WINDOWS\system32\apphelp.dll
 Opens:
                         C:\WINDOWS\AppPatch\sysmain.sdb
                         C:\WINDOWS\AppPatch\systest.sdb
 Opens:
 Opens:
                         C:\WINDOWS\Temp
 Opens:
                         C:\
                         C:\WINDOWS
 Opens:
                         C:\windows\temp\6b78f38317a53920e530cc1e36053242.exe.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\shell32.dll
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Manifest
                         C:\WINDOWS\system32\SHELL32.dll.124.Config
 Opens:
 Opens:
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
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:
 Opens:
                         C:\WINDOWS\WindowsShell.Config
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Config
                         C:\WINDOWS\system32\WININET.dll.123.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\WININET.dll.123.Config
 Opens:
                         C:\WINDOWS\system32\ws2_32.dll
                         C:\WINDOWS\system32\ws2help.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\advpack.dll
 Opens:
                         C:\WINDOWS\system32\setupapi.dll
 Opens:
                         C:\WINDOWS\system32\kernel32.dll
 Opens:
                         C:\WINDOWS\system32\ntdll.dll
 Opens:
                         C:\WINDOWS\system32\advapi32.dll
 Opens:
                         C:\Program Files\Bifrost\server.exe
 Opens:
                         C:\Program Files\Bifrost
 Opens:
                         C:\Program Files\Bifrost\logg.dat
                         C:\Program Files\Internet Explorer\iexplore.exe
 Opens:
 Opens:
                         C:\Program Files\Internet Explorer
 Opens:
                         C:\Program Files\Internet Explorer\IEXPLORE.EXE.Manifest
 Opens:
                         C:\WINDOWS\Prefetch\IEXPLORE.EXE-27122324.pf
 Opens:
 Opens:
                         C:\Documents and Settings
                         C:\Documents and Settings\Admin\Cookies
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\History\History.IE5}
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X
                         C:\WINDOWS\system32\calc.exe
 Opens:
 Opens:
                         C:\Program Files
 Opens:
                         C:\WINDOWS\Registration
 Opens:
                         C:\WINDOWS\system32
 Opens:
                         C:\WINDOWS\system32\en-US
 Opens:
                         C:\WINDOWS\WinSxS
 Opens:
                         C:\WINDOWS\system32\unicode.nls
 Opens:
                         C:\WINDOWS\system32\locale.nls
                         C:\WINDOWS\system32\sorttbls.nls
 Opens:
 Opens:
                         C:\WINDOWS\svstem32\rpcrt4.dll
 Opens:
                         C:\WINDOWS\system32\secur32.dll
                         C:\WINDOWS\system32\user32.dll
 Opens:
                         C:\WINDOWS\system32\gdi32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\msvcrt.dll
 Opens:
                         C:\WINDOWS\system32\shlwapi.dll
 Opens:
                         C:\WINDOWS\system32\ole32.dll
 Opens:
                         C:\WINDOWS\system32\iertutil.dll
 Opens:
                         C:\WINDOWS\system32\urlmon.dll
 Opens:
                         C:\WINDOWS\system32\oleaut32.dll
 Opens:
                         C:\WINDOWS\system32\ctype.nls
 Opens:
                         C:\WINDOWS\system32\sortkey.nls
                         C:\WINDOWS\system32\ieframe.dll
 Opens:
```

```
C:\WINDOWS\system32\en-US\ieframe.dll.mui
 Opens:
 Opens:
                         C:\WINDOWS\system32\comdlg32.dll
 Opens:
                         C:\WINDOWS\system32\rpcss.dll
 Opens:
                         C:\Program Files\Internet Explorer\sqmapi.dll
 Opens:
                         C:\WINDOWS\system32\winlogon.exe
 Opens:
                         C:\WINDOWS\system32\xpsp2res.dll
                         C:\WINDOWS\system32\clbcatq.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\comres.dll
 Opens:
                         C:\WINDOWS\system32\version.dll
                         C:\WINDOWS\Registration\R00000000007.clb
 Opens:
 Opens:
                         C:\Program Files\Internet Explorer\ieproxy.dll
 Opens:
                         C:\WINDOWS\system32\wininet.dll
 Opens:
                         C:\WINDOWS\system32\normaliz.dll
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\index.dat
                         C:\Documents and Settings\Admin\Cookies\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\index.dat
 Opens:
                         C:\WINDOWS\system32\mlang.dll
 Opens:
                         C:\WINDOWS\system32\uxtheme.dll
 Opens:
                         C:\WINDOWS\system32\sxs.dll
 Opens:
                         C:\WINDOWS\system32\actxprxy.dll
 Opens:
                         C:\WINDOWS\system32\rasapi32.dll
 Opens:
                         C:\WINDOWS\system32\rasman.dll
 Opens:
                         C:\WINDOWS\system32\netapi32.dll
                         C:\WINDOWS\system32\tapi32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\rtutils.dll
 Opens:
                         C:\WINDOWS\system32\userenv.dll
                         C:\WINDOWS\system32\sensapi.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\msv1_0.dll
 Opens:
                         C:\WINDOWS\system32\iphlpapi.dll
 Opens:
                         C:\WINDOWS\system32\narrhook.dll
 Opens:
                         C:\WINDOWS\system32\oleacc.dll
 Opens:
                         C:\WINDOWS\system32\msvcp60.dll
 Opens:
                         C:\WINDOWS\system32\oleaccrc.dll
 Opens:
                         C:\WINDOWS\system32\MSIMTF.dll
 Opens:
                         C:\WINDOWS\system32\stdole2.tlb
 Opens:
                         C:\WINDOWS\system32\msimg32.dll
 Opens:
                         C:\WINDOWS\system32\ntkrnlpa.exe
 Opens:
                         C:\WINDOWS\system32\avicap32.dll
                         C:\WINDOWS\system32\msvfw32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\mswsock.dll
 Opens:
                         C:\WINDOWS\system32\dnsapi.dll
                         C:\WINDOWS\system32\winrnr.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\drivers\etc\hosts
 Opens:
                         C:\WINDOWS\system32\rsaenh.dll
                         C:\WINDOWS\system32\crypt32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\hnetcfg.dll
 Opens:
                         C:\WINDOWS\system32\wshtcpip.dll
                         {\tt C:\WINDOWS\system32\rasadhlp.dll}\\
 Opens:
```

Writes to: C:\Program Files\Bifrost\server.exe Reads from:

C:\WINDOWS\Temp\6b78f38317a53920e530cc1e36053242.exe Reads from:

C:\WINDOWS\system32\kernel32.dll Reads from: C:\WINDOWS\system32\ntdll.dll Reads from: C:\WINDOWS\svstem32\advapi32.dll

C:\WINDOWS\Prefetch\IEXPLORE.EXE-27122324.pf Reads from:

Reads from: C:\Program Files\Bifrost\server.exe Reads from: C:\WINDOWS\system32\calc.exe Reads from: C:\WINDOWS\system32\avicap32.dll Reads from: C:\WINDOWS\system32\drivers\etc\hosts C:\WINDOWS\system32\rsaenh.dll

Network Events

DNS query: probook.zapto.org

DNS response: probook.zapto.org \Rightarrow 5.15.116.86

Connects to: 5.15.116.86:1800 Sends data to: 8.8.8.8:53 Receives data from: 0.0.0.0:0

Windows Registry Events

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

folders

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

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

Creates key: HKLM\software\microsoft\active setup\installed components\{9d71d88c-

c598-4935-c5d1-43aa4db90836}

Creates key: HKLM\software\bifrost Creates key: HKCU\software\bifrost HKCU\sessioninformation Creates key:

Creates key: HKLM\system\currentcontrolset\control\mediaresources\msvideo Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters

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

options\6b78f38317a53920e530cc1e36053242.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\currentcontrolset\control\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

 $options \verb|\rpcrt4.dll|$

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\version.dll

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

options\comctl32.dll

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

options\winmm.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: ${\tt HKLM\backslash software\backslash microsoft\backslash windows\ nt\backslash current version\backslash diagnostics}$

Opens key: HKLM\software\microsoft\ole

Opens key: HKCR\interface

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

Opens key: HKLM\software\microsoft\oleaut

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

Opens key: HKCU\

Opens key: ${\tt HKCU \setminus software \setminus policies \setminus microsoft \setminus control\ panel \setminus desktop}$

Opens key: HKCU\control panel\desktop

Opens key: $\hspace{1.5cm} \hspace{1.5cm} \hspace{1.5cm$

Opens key:

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

Opens key: HKCU\software\borland\locales
Opens key: HKLM\software\borland\locales
Opens key: HKCU\software\borland\delphi\locales

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

options\msctf.dll

Opens key:

 $HKLM \setminus software \setminus microsoft \setminus ctf \setminus compatibility \setminus 6b78f38317a53920e530cc1e36053242. exercise the software \setminus microsoft \setminus ctf \setminus compatibility \setminus 6b78f38317a53920e530cc1e36053242. exercise the software \setminus microsoft \setminus ctf \setminus compatibility \setminus 6b78f38317a53920e530cc1e36053242. exercise the software \setminus microsoft \setminus ctf \setminus compatibility \setminus 6b78f38317a53920e530cc1e36053242. exercise the software \setminus microsoft \setminus ctf \setminus compatibility \setminus 6b78f38317a53920e530cc1e36053242. exercise the software \setminus microsoft \setminus ctf \setminus compatibility \setminus 6b78f38317a53920e530cc1e36053242. exercise the software \setminus microsoft \setminus ctf \setminus compatibility \setminus 6b78f38317a53920e530cc1e36053242. exercise the software \setminus microsoft \setminus ctf \setminus compatibility \setminus 6b78f38317a53920e530cc1e36053242. exercise the software \setminus microsoft \setminus ctf \setminus compatibility \setminus ctf \setminus ct$

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\imm

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: HKLM\software\microsoft\ctf\systemshared

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

 $Opens\ key: \\ HKLM\software\microsoft\windows\ nt\currentversion\app compatflags\layers$

Opens key: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags\custom\6b78f38317a53920e530cc1e36053242.exe

Opens key: HKLM\software\policies\microsoft\windows\safer\levelobjects
Opens key: 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: b813f72dbb91} Opens key: 7c29ddecae3f} Opens key: $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ has hes \ \{94e3e076-8f53-42a5-8411-64444, not windows \ has he should be a substitute of the same between the$ 085bcc18a68d} Opens key: b91490411bfc} Opens key: $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus urlzones$ Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes Opens key: $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus urlzones$ Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths Opens kev: $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus has hes$ Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes Opens kev: Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \normallows \policies \microsoft \normallows \policies \p$ Opens kev: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \norm{\backslash hashes} \end{tabular}$ Opens key: Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \normallows \end{tabular} \begin{tabular}{ll} Akcular \normallows \normallows$ Opens kev: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths Opens kev: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes Opens key: $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus urlzones$ Opens kev: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones Opens key: $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus paths$ Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones Opens key: $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus paths$ Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes Opens key:

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

HKCU\software\microsoft\windows\currentversion\explorer\shell folders Opens kev: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shlwapi.dll

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

options\shell32.dll

Opens kev: HKLM\system\setup

Opens key:

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\normaliz.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\iertutil.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: options\urlmon.dll Opens key: HKCU\software\classes\ HKCU\software\classes\protocols\name-space handler\ Opens key: Opens key: HKCR\protocols\name-space handler Opens key: HKCU\software\classes\protocols\name-space handler Opens key: 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 HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\ Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol HKCU\software\policies\microsoft\internet explorer\main\featurecontrol Opens key: Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ settings\zonemap\domains\ HKCU\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zonemap\domains\ Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\ Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\ HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_unc_savedfilecheck Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\wininet.dll Opens key: HKLM\system\currentcontrolset\control\wmi\security HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\ws2help.dll Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$ options\ws2_32.dll Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution options\setupapi.dll Opens key: HKLM\system\currentcontrolset\control\minint HKLM\system\wpa\pnp Opens key: Opens key: HKLM\software\microsoft\windows\currentversion\setup HKLM\software\microsoft\windows\currentversion Opens key: Opens key: HKLM\software\microsoft\windows\currentversion\setup\apploglevels Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters Opens key: HKLM\software\policies\microsoft\system\dnsclient HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\advpack.dll Opens key: HKLM\software\microsoft\advanced inf setup Opens key: HKLM\software\microsoft\active setup\installed components\<{12d0ed0d-Opens key: 0ee0-4f90-8827-78cefb8f4988} Opens key: b0f6-11d0-94ab-0080c74c7e95} HKLM\software\microsoft\active setup\installed components\>{26923b43-Opens key: 4d38-484f-9b9e-de460746276c} Opens key: c7cc-11d0-8953-00a0c90347ff} Opens key: HKLM\software\microsoft\active setup\installed components\>{60b49e34c7cc-11d0-8953-00a0c90347ff}micros HKLM\software\microsoft\active setup\installed components\>{881dd1c5-Opens kev: 3dcf-431b-b061-f3f88e8be88a} Opens key: 4fcb-11cf-aaa5-00401c608500} Opens key: HKLM\software\microsoft\active setup\installed components\{10072cec-8cc1-11d1-986e-00a0c955b42f} Opens key: HKLM\software\microsoft\active setup\installed components\{2179c5d3ebff-11cf-b6fd-00aa00b4e220} Opens key: HKLM\software\microsoft\active setup\installed components\{22d6f312b0f6-11d0-94ab-0080c74c7e95} Opens key:

```
2c60-11d0-a31d-00aa00b92c03}
                                                                                                                             HKLM\software\microsoft\active setup\installed components\{2c7339cf-
         Opens kev:
2b09-4501-b3f3-f3508c9228ed}
         Opens key:
                                                                                                                             HKLM\software\microsoft\active setup\installed components\{36f8ec70-
c29a-11d1-b5c7-0000f8051515}
         Opens key:
                                                                                                                             a269-11d1-b5bf-0000f8051515}
                                                                                                                             HKLM \ software \ microsoft \ active \ setup \ installed \ components \ \ \{3bf42070-microsoft\} \ description \ descrip \ description \ description \ description \ description \ descr
        Opens key:
b3b1-11d1-b5c5-0000f80515153
         Opens key:
                                                                                                                             HKLM\software\microsoft\active setup\installed components\{4278c270-
a269-11d1-b5bf-0000f8051515}
         Opens key:
                                                                                                                             HKLM \ software \ microsoft \ active \ setup \ installed \ components \ \ \{44bba840-microsoft \ active \ setup \ active \ ac
cc51-11cf-aafa-00aa00b6015c}
        Opens key:
                                                                                                                             HKLM\software\microsoft\active setup\installed components\{44bba842-
 cc51-11cf-aafa-00aa00b6015b}
                                                                                                                             HKLM\software\microsoft\active setup\installed components\{44bba848-
         Opens key:
cc51-11cf-aafa-00aa00b6015c}
                                                                                                                             HKLM\software\microsoft\active setup\installed components\{44bba855-
         Opens key:
cc51-11cf-aafa-00aa00b6015f}
                                                                                                                             HKLM \ software \ microsoft \ active \ setup \ installed \ components \ \ \{45ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-1645ea75a0-16
        Opens key:
 a269-11d1-b5bf-0000f8051515}
                                                                                                                             HKLM\software\microsoft\active setup\installed components\{4f216970-
         Opens key:
c90c-11d1-b5c7-0000f8051515}
                                                                                                                             HKLM\software\microsoft\active setup\installed components\{4f645220-
         Opens key:
306d-11d2-995d-00c04f98bbc9}
                                                                                                                             Opens key:
 1e7d-11d1-bc44-00c04fd912be}
         Opens key:
                                                                                                                             HKLM\software\microsoft\active setup\installed components\{5a8d6ee0-
3e18-11d0-821e-444553540000}
                                                                                                                             HKLM\software\microsoft\active setup\installed components\{5fd399c0-
         Opens key:
a70a-11d1-9948-00c04f98bbc9}
                                                                                                                             HKLM\software\microsoft\active setup\installed components\{630b1da0-
         Opens key:
b465-11d1-9948-00c04f98bbc9}
         Opens key:
                                                                                                                             HKLM\software\microsoft\active setup\installed components\{6bf52a52-
394a-11d3-b153-00c04f79faa6}
                                                                                                                             \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} in stalled components \end{tabular} $$ (6fab 99d 0-1) $$ (100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 10
         Opens key:
bab8-11d1-994a-00c04f98bbc9}
         Opens key:
                                                                                                                             HKLM\software\microsoft\active setup\installed components\{7790769c-
0471-11d2-af11-00c04fa35d02}
                                                                                                                             HKLM\software\microsoft\active setup\installed components\{89820200-
         Opens key:
 ecbd-11cf-8b85-00aa005b4340}
         Opens key:
                                                                                                                             HKLM\software\microsoft\active setup\installed components\{89820200-
ecbd-11cf-8b85-00aa005b4383}
         Opens key:
                                                                                                                             HKLM\software\microsoft\active setup\installed components\{89b4c1cd-
b018-4511-b0a1-5476dbf70820}
                                                                                                                             HKLM\software\microsoft\active setup\installed components\{9381d8f2-
         Opens key:
0288-11d0-9501-00aa00b911a5}
         Opens key:
                                                                                                                             4266-43f0-b6ed-9d38c4202c7e}
         Opens key:
                                                                                                                             HKLM\software\microsoft\active setup\installed components\{c09fb3cd-
 3d0c-3f2d-899a-6a1d67f2073f}
                                                                                                                             HKLM\software\microsoft\active setup\installed components\{c9e9a340-
        Opens key:
d1f1-11d0-821e-444553540600}
         Opens key:
                                                                                                                             HKLM \ software \ microsoft \ active \ setup \ installed \ components \ \ \{cc2a9ba0-microsoft\} \ description \ descrip \ description \ description \ description \ description \ descr
3bdd-11d0-821e-444553540000}
         Opens key:
                                                                                                                             HKLM\software\microsoft\active setup\installed components\{cdd7975e-
 60f8-41d5-8149-19e51d6f71d0}
                                                                                                                             HKLM\software\microsoft\active setup\installed components\{d27cdb6e-
         Opens key:
 ae6d-11cf-96b8-444553540000}
                                                                                                                             HKLM\software\microsoft\active setup\installed components\{de5aed00-
         Opens key:
 a4bf-11d1-9948-00c04f98bbc9}
        Opens key:
                                                                                                                             b707-11d2-9cbd-0000f87a369e}
                                                                                                                             HKCU\software\microsoft\active setup\installed components\{9d71d88c-
         Opens kev:
 c598-4935-c5d1-43aa4db90836}
         Opens kev:
                                                                                                                             HKLM\system\currentcontrolset\control\computername
         Opens key:
                                                                                                                             HKCR\http\shell\open\command
         Opens key:
                                                                                                                             \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
 options\iexplore.exe
         Opens kev:
                                                                                                                             HKCU\software\classes\applications\calc.exe
         Opens key:
                                                                                                                             HKCR\applications\calc.exe
         Opens key:
                                                                                                                             HKCU\software\microsoft\windows\shellnoroam\muicache\
         Opens key:
                                                                                                                             HKLM\software\microsoft\windows\currentversion\explorer\fileassociation
         Opens key:
                                                                                                                             HKLM\software\microsoft\ctf\tip\
         Opens key:
                                                                                                                             HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
c9633f71be64}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}
                                                                                                                             HKLM \setminus software \setminus icrosoft \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-4fcc
         Opens key
 77e8f3d1aa80}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}
                                                                                                                             HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
        Opens key:
 c9633f71be64}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}
         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\} \verb|\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31\}| 
         Opens key:
                                                                                                                             HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
```

```
c9633f71be64}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
                                          HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
  Opens key
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
                                          HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
   Opens key:
c9633f71be64\\ \\ category\\ \\ item\\ \\ \{7ae86bb7-262c-431e-9111-c974b6b7cac3\}
  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\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
                                          HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
  Opens key:
c9633f71be64}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}
   Opens key:
                                          HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}
   Opens key:
                                          HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
\verb|c9633f71be64| \land \verb|category| item| \{c6debc0a-f2b2-4f17-930e-ca9faff4cd04\}| \\
                                          HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
  Opens key:
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
   Opens key:
                                          HKLM\software\microsoft\rpc\pagedbuffers
   Opens kev:
                                          HKIM\software\microsoft\rpc
   Opens key:
                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iexplore.exe\rpcthreadpoolthrottle
                                         HKLM\software\policies\microsoft\windows nt\rpc
   Opens key:
   Opens key:
                                          HKLM\software\microsoft\ctf\compatibility\iexplore.exe
   Opens key:
                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvfw32.dll
   Opens key:
                                          HKLM\software\microsoft\windows nt\currentversion\vfw
   Opens key:
                                          HKLM\system\currentcontrolset\control\mediaresources\msvideo
                                          HKLM\system\currentcontrolset\services\winsock2\parameters
   Opens key:
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
   Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001
   Opens kev:
Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000004
   Opens key:
Opens kev:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
   Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
   Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010
   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 key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
  Opens key:
                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mswsock.dll
   Opens key:
                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dnsapi.dll
   Opens key:
                                          HKLM\system\currentcontrolset\services\dnscache\parameters
   Opens key:
                                          HKLM\software\policies\microsoft\windows nt\dnsclient
   Opens key:
                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iphlpapi.dll
   Opens key:
                                          HKLM\system\currentcontrolset\services\tcpip\linkage
   Opens kev:
                                          HKLM\svstem\currentcontrolset\services\tcpip\parameters\
   Opens key:
                                          HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
   Opens kev:
                                          HKLM\system\currentcontrolset\services\netbt\parameters
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}
   Opens kev:
                                          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 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 key: HKLM\software\policies\microsoft\cryptography

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

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

options\hnetcfg.dll

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

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

options\wshtcpip.dll

Opens key:

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

options\rasadhlp.dll

Opens key: $\label{lem:hkcu-appevents-schemes-apps-lemontification-current} \\ \text{Hkcu-appevents-schemes-apps-lemontification-current} \\ \\ \text{Hkcu-app-lemontification-current} \\ \\ \text{Hkcu-app-lemontification-current} \\ \\ \text{Hkcu-app-lemontification-current} \\ \\ \text{Hkcu-app-lemontification-current} \\ \\ \\ \text{Hkcu-app-lemontification-current} \\ \\ \\ \\ \text{Hkcu-app-lemontification-current} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\$

Opens key: HKLM\software\microsoft\com3

Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}

HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e} Opens kev: Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-

00805fc1270e}\treatas

HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-

00805fc1270e}\inprocserver32

HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprocserver32 Opens kev:

Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-

00805fc1270e}\inprocserverx86

HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprocserverx86 Opens key:

Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-

00805fc1270e}\localserver32

HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\localserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-

00805fc1270e}\inprochandler32

 $HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\{\inprochandler32}$ Opens key:

Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-

00805fc1270e}\inprochandlerx86

 $HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\\\\$ Opens key:

Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-

00805fc1270e}\localserver

HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\localserver Opens key: Opens key: HKCU\software\classes\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}

Opens key: HKCR\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}

Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{33c4643c-7811-46fa-a89a-768597bd7223\}$

Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223} HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-Opens kev:

768597bd7223}\treatas

HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\treatas Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-Opens key:

768597bd7223}\inprocserver32

 $HKCR \ clsid \ \{33c4643c-7811-46fa-a89a-768597bd7223\} \ \ inprocserver 32$ Opens key:

Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-

768597bd7223}\inprocserverx86

HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserverx86 Opens key:

HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-Opens key:

768597bd7223}\localserver32

Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\localserver32

Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-

768597bd7223}\inprochandler32

HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprochandler32 Opens key:

Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-

768597bd7223}\inprochandlerx86

HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprochandlerx86 Opens kev:

Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-

768597bd7223}\localserver

Opens key: $\label{localserver} $HKCR\clsid{33c4643c-7811-46fa-a89a-768597bd7223} \le e^{-7811-46fa-a89a-768597bd7223} \le e^{-7811-46fa-a89a-768597bd7223}$ HKCU\software\policies\microsoft\windows\network connections Opens kev: HKLM\software\policies\microsoft\windows\network connections Opens key: HKCU\software\classes\clsid\{2227a280-3aea-1069-a2de-Opens key:

08002b30309d}\shellfolder

 $HKCR \ clsid \ \{2227a280-3aea-1069-a2de-08002b30309d\} \ shell folder$ Opens key:

Opens key: $HKCU \ software \ microsoft \ windows \ current version \ explorer \ clsid \ \{2227a280-microsoft\} \ description \ description$

3aea-1069-a2de-08002b30309d}

Opens key: HKCU\software\microsoft\windows\currentversion\policies\nonenum HKLM\software\microsoft\windows\currentversion\policies\nonenum Opens kev: Opens key:

HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{2227a280-3aea-1069-

a2de-08002b30309d}

Opens kev: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \clsid \cline{2227a280-microsoft} \end{tabular}$

3aea-1069-a2de-08002b30309d}\shellfolder

```
Opens key:
                                                 HKLM \ software \ `microsoft\ `windows \ `current version \ `explorer\ `clsid\ `\{2227a280-microsoft\ `windows\ `current version\ `explorer\ `clsid\ `\{2227a280-microsoft\ `windows\ `current version\ `explorer\ `clsid\ `\{2227a280-microsoft\ `windows\ `current version\ `explorer\ `clsid\ `all `all `explorer\ `clsid\ `explorer\ `clsid\ `all `explorer\ `clsid\ `all `explorer\ `clsid\ `explorer\ `explorer\ `clsid\ `explorer\ `explore
3aea-1069-a2de-08002b30309d}\shellfolder
   Opens key:
                                                 HKCU\software\classes\clsid\{2227a280-3aea-1069-a2de-08002b30309d}
   Opens key:
                                                 HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}
                                                 HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}\
   Opens key:
   Opens key:
                                                 HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}\shellfolder
                                                 HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\shellfolder
   Opens key:
   Opens key:
                                                 HKCU\software\microsoft\windows\currentversion\explorer\clsid\{7007acc7-
3202-11d1-aad2-00805fc1270e}
   Opens kev:
HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ objects \ \{7007acc7-3202-11d1-1244\} \ objects \ for the sum of the sum o
aad2-00805fc1270e}
                                                 Opens key:
3202-11d1-aad2-00805fc1270e}\shellfolder
   Opens key:
                                                 HKLM\software\microsoft\windows\currentversion\explorer\clsid\{7007acc7-
3202-11d1-aad2-00805fc1270e}\shellfolder
   Opens key:
                                                 HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}
   Opens key:
                                                 HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}
                                                 HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\
   Opens key:
   Queries value:
                                                 HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
                                                 HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
   Queries value:
                                                 HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\gre_initialize[disablemetafiles]
                                                 HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\compatibility32[6b78f38317a53920e530cc1e36053242]
   Oueries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[6b78f38317a53920e530cc1e36053242]
                                                 HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
   Oueries value:
   Queries value:
                                                 HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
                                                 HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
   Queries value:
   Queries value:
                                                 HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
                                                 HKLM\software\microsoft\ole[rwlockresourcetimeout]
   Queries value:
                                                 HKCR\interface[interfacehelperdisableall]
   Oueries value:
   Oueries value:
                                                 HKCR\interface[interfacehelperdisableallforole32]
                                                 HKCR\interface[interfacehelperdisabletypelib]
   Queries value:
                                                 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:
                                                 HKCU\control panel\desktop[smoothscroll]
   Queries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
   Oueries value:
                                                 HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 1]
   Queries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
   Oueries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
   Oueries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
   Oueries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
   Oueries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
   Oueries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
   Queries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
   Oueries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
   Queries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
   Oueries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
   Oueries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
   Oueries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
   Queries value:
   Queries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
   Oueries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
   Queries value:
   Queries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
   Oueries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
   Oueries value:
```

HKLM\software\microsoft\windows nt\currentversion\drivers32[aux] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1] Oueries value: $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [aux 2]$ Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9] Oueries value:

HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer] HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1] Oueries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]

Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]

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\software\microsoft\windows nt\currentversion\imm[ime file]
Queries value: HKCU\software\microsoft\ctf[disable thread input manager]

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

manager[safeprocesssearchmode]

 $\label{thm:current} Queries \ value: \\ HKLM\system\currentcontrolset\control\session$

manager\appcompatibility[disableappcompat]

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

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

Queries value:

 $HKLM software \\policies \\microsoft \\windows \\safer \\code identifiers \\0 \\paths \\dda3f824-d8cb-441b-834d-be2efd2c1a33\\fitem \\data]$

Queries value:

Queries value:

 $HKLM software \\policies \\microsoft \\windows \\safer \\code identifiers \\0 \\hashes \\\{349d35ab-37b5-462f-9b89-edd5fbde \\1328\} \\[itemdata]$

Oueries value:

Queries value:

Queries value:

 $HKLM software \\policies \\microsoft \\windows \\safer \\code identifiers \\0 \\hashes \\\{349d35ab-37b5-462f-9b89-edd5fbde \\1328\} \\ \\range \\large \\l$

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

Queries value:

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

Queries value:

Queries value:

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \policies \microsoft \windows \safer \code identifiers \oldshes \{94e3e076-8f53-42a5-8411-085bcc18a68d\} [saferflags]$

Queries value:

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

Queries value:

Queries value:

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

Queries value:

```
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe
b91490411bfc}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
   Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
   Oueries value:
                                              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
                                              HKLM\system\setup[systemsetupinprogress]
   Oueries value:
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
   Oueries value:
                                              HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
                                              HKLM\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_protocol_lockdown[6b78f38317a53920e530cc1e36053242.exe]
   Queries value:
                                              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
                                              HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
   Queries value:
ab78-1084642581fb]
   Queries value:
                                               HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
0000-0000000000001
   Queries value:
                                               HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
   Queries value:
                                               HKLM\system\wpa\pnp[seed]
                                               HKLM\system\setup[osloaderpath]
   Queries value:
   Queries value:
                                               HKLM\system\setup[systempartition]
   Oueries 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]
   Queries value:
                                              HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
   Oueries value:
                                              HKLM\software\microsoft\windows\currentversion[devicepath]
                                               HKLM\software\microsoft\windows\currentversion\setup[loglevel]
   Queries value:
                                              HKLM\software\microsoft\windows\currentversion\setup[logpath]
   Oueries value:
   Oueries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
                                              HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
   Queries value:
   Queries value:
                                              HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
                                               HKLM\software\microsoft\advanced inf setup[advpacklogfile]
   Queries value:
   Oueries value:
                                              HKLM\software\microsoft\active setup\installed components\<{12d0ed0d-
0ee0-4f90-8827-78cefb8f4988}[stubpath]
                                               HKLM\software\microsoft\active setup\installed components\>{22d6f312-
   Oueries value:
b0f6-11d0-94ab-0080c74c7e95}[stubpath]
   Queries value:
                                              \label{lem:hklmsoftware} HKLM \software \microsoft \software \so
4d38-484f-9b9e-de460746276c}[stubpath]
                                              HKLM\software\microsoft\active setup\installed components\>{60b49e34-
   Oueries value:
c7cc-11d0-8953-00a0c90347ff}[stubpath]
   Oueries value:
                                              HKLM\software\microsoft\active setup\installed components\>{60b49e34-
c7cc-11d0-8953-00a0c90347ff}micros[stubpath]
   Queries value:
                                              HKLM\software\microsoft\active setup\installed components\>{881dd1c5-
3dcf-431b-b061-f3f88e8be88a}[stubpath]
                                              HKLM\software\microsoft\active setup\installed components\{08b0e5c0-
   Oueries value:
4fcb-11cf-aaa5-00401c608500}[stubpath]
   Queries value:
                                              HKLM\software\microsoft\active setup\installed components\{10072cec-
8cc1-11d1-986e-00a0c955b42f}[stubpath]
   Queries value:
                                              HKLM\software\microsoft\active setup\installed components\{2179c5d3-
ebff-11cf-b6fd-00aa00b4e220}[stubpath]
                                              HKLM\software\microsoft\active setup\installed components\{22d6f312-
   Queries value:
b0f6-11d0-94ab-0080c74c7e95}[stubpath]
   Queries value:
                                               HKLM\software\microsoft\active setup\installed components\{283807b5-
2c60-11d0-a31d-00aa00b92c03}[stubpath]
   Queries value:
                                              HKLM\software\microsoft\active setup\installed components\{2c7339cf-
2b09-4501-b3f3-f3508c9228ed}[stubpath]
                                              HKLM\software\microsoft\active setup\installed components\{36f8ec70-
   Queries value:
c29a-11d1-b5c7-0000f8051515}[stubpath]
   Queries value:
                                              HKLM\software\microsoft\active setup\installed components\{3af36230-
a269-11d1-b5bf-0000f8051515}[stubpath]
   Queries value:
                                              HKLM\software\microsoft\active setup\installed components\{3bf42070-
b3b1-11d1-b5c5-0000f8051515}[stubpath]
                                              HKLM\software\microsoft\active setup\installed components\{4278c270-
   Oueries value:
a269-11d1-b5bf-0000f8051515}[stubpath]
   Queries value:
                                              HKLM\software\microsoft\active setup\installed components\{44bba840-
cc51-11cf-aafa-00aa00b6015c}[stubpath]
   Queries value:
                                              HKLM\software\microsoft\active setup\installed components\{44bba842-
cc51-11cf-aafa-00aa00b6015b}[stubpath]
                                              HKLM\software\microsoft\active setup\installed components\{44bba848-
   Oueries value:
cc51-11cf-aafa-00aa00b6015c}[stubpath]
   Queries value:
                                              HKLM\software\microsoft\active setup\installed components\{44bba855-
cc51-11cf-aafa-00aa00b6015f}[stubpath]
```

 $HKLM \ software \ microsoft \ active \ setup \ installed \ components \ \ \{45ea75a0-16$

Queries value:

```
a269-11d1-b5bf-0000f8051515}[stubpath]
                                                       HKLM\software\microsoft\active setup\installed components\{4f216970-
    Oueries value:
c90c-11d1-b5c7-0000f8051515}[stubpath]
    Queries value:
                                                       HKLM\software\microsoft\active setup\installed components\{4f645220-
306d-11d2-995d-00c04f98bbc9}[stubpath]
    Queries value:
                                                       HKLM\software\microsoft\active setup\installed components\{5945c046-
1e7d-11d1-bc44-00c04fd912be}[stubpath]
    Oueries value:
                                                       HKLM\software\microsoft\active setup\installed components\{5a8d6ee0-
3e18-11d0-821e-444553540000}[stubpath]
    Queries value:
                                                       HKLM\software\microsoft\active setup\installed components\{5fd399c0-
a70a-11d1-9948-00c04f98bbc9}[stubpath]
                                                       HKLM\software\microsoft\active setup\installed components\{630b1da0-
    Queries value:
b465-11d1-9948-00c04f98bbc9}[stubpath]
    Oueries value:
                                                       HKLM\software\microsoft\active setup\installed components\{6bf52a52-
394a-11d3-b153-00c04f79faa6}[stubpath]
    Queries value:
                                                       HKLM\software\microsoft\active setup\installed components\{6fab99d0-
bab8-11d1-994a-00c04f98bbc9}[stubpath]
                                                       HKLM\software\microsoft\active setup\installed components\{7790769c-
    Queries value:
0471-11d2-af11-00c04fa35d02}[stubpath]
                                                       HKLM\software\microsoft\active setup\installed components\{89820200-
    Queries value:
ecbd-11cf-8b85-00aa005b4340}[stubpath]
    Queries value:
                                                       HKLM\software\microsoft\active setup\installed components\{89820200-
echd-11cf-8b85-00aa005b4383}[stubpath]
                                                       HKLM\software\microsoft\active setup\installed components\{89b4c1cd-
    Queries value:
b018-4511-b0a1-5476dbf70820}[stubpath]
                                                       Queries value:
0288-11d0-9501-00aa00b911a5}[stubpath]
    Queries value:
                                                       HKLM\software\microsoft\active setup\installed components\{acc563bc-
4266-43f0-b6ed-9d38c4202c7e}[stubpath]
                                                       \label{lem:hklm} \begin{tabular}{ll} HKLM \end{tabular} in the components \end{tabular} $$ (c09fb3cd-t) $$ (c09fb3cd-t) $$ (constant) $$ (co
    Queries value:
3d0c-3f2d-899a-6a1d67f2073f}[stubpath]
                                                       Queries value:
d1f1-11d0-821e-444553540600}[stubpath]
    Queries value:
                                                       HKLM\software\microsoft\active setup\installed components\{cc2a9ba0-
3bdd-11d0-821e-444553540000}[stubpath]
                                                       \label{lem:hklmsoftware} \begin{tabular}{l} HKLM \software \microsoft \active setup \slightly installed components \cite{lem:hklmsoftware} \end{tabular} \begin{tabular}{l} Active setup \slightly installed \cite{lem:hklmsoftware} \end{tabular} \begin{tabular}{l} Active setup \slightly installed \cite{lem:hklmsoftware} \end{tabular} \begin{tabular}{l} Active setup \cite{lem:hklmsoftware} \end{tabular} \begin{tabular}{l} Active
    Queries value:
60f8-41d5-8149-19e51d6f71d0}[stubpath]
    Oueries value:
                                                       HKLM\software\microsoft\active setup\installed components\{d27cdb6e-
ae6d-11cf-96b8-444553540000}[stubpath]
    Queries value:
                                                       \label{lem:hklmsoftware} HKLM \ software \ \ setup\ \ installed \ components \ \ \ \{de5 a ed00-de5 a ed00-de
a4bf-11d1-9948-00c04f98bbc9}[stubpath]
    Queries value:
                                                       HKLM\software\microsoft\active setup\installed components\{e92b03ab-
b707-11d2-9cbd-0000f87a369e}[stubpath]
    Queries value:
                                                       HKLM\software\microsoft\windows\currentversion[programfilesdir]
                                                       HKLM\software\bifrost[nck]
    Oueries value:
    Queries value:
                                                       HKCR\http\shell\open\command[]
    Queries value:
HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\calc.exe]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\fileassociation[cutlist]
    Oueries value:
                                                       HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}[dword]
    Queries value:
                                                       HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}[dword]
                                                       HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
   Oueries value:
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}[dword]
    Oueries value:
                                                       HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[dword]
    Oueries value:
                                                       HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}[dword]
                                                       HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
   Queries value:
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}[dword]
    Queries value:
                                                       HKLM\software\microsoft\windows
nt\currentversion\compatibilitv32\iexplore1
    Queries value:
                                                       HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[iexplore]
                                                       HKLM\software\microsoft\internet
    Queries value:
explorer\main\featurecontrol\feature_protocol_lockdown[iexplore.exe]
    Queries value:
                                                       HKLM\software\microsoft\rpc[maxrpcsize]
    Oueries value:
                                                       HKCU\software\bifrost[plg1]
    Queries value:
                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo]
    Oueries value:
                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo1]
    Oueries value:
                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo2]
    Queries value:
                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo3]
    Queries value:
                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo4]
    Oueries value:
                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo51
    Queries value:
                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo6]
    Oueries value:
                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo7]
    Oueries value:
                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo81
    Oueries value:
                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo9]
    Queries value:
```

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

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

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem] Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries \ 0000000000008 \ [packed catalog item] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
 Queries value:
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
- Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries \ 000000000011 \ [packed catalog item] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 000000000001 \ [displaystring] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[supportednamespace] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[storesserviceclassinfo]

 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
 - Queries value:
- $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws 2_32 spin count]$

```
Oueries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [prioritize record data]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
 Oueries value:
                        HKLM\system\currentcontrolset\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\dnscache\parameters[registrationenabled]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [register primary name]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
 Oueries value:
Queries value:
Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
 Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
 Queries value:
                        HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
                        HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
 Oueries value:
 Oueries value:
                        HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
 Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [multicastlisten level]
```

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

c7d49d7cecdc}[enabledhcp]

Oueries value:

 $\label{thm:local_equation} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$ HKLM \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$ \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$$ \end{tabular} $$ \end{tabular} $$$ \end{tabular} $$ \end{tabular} $$$ \end{tabular} $$$ \end{tabular} $$ c7d49d7cecdc}[leaseobtainedtime]

c7d49d7cecdc}[leaseterminatestime]

Oueries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-4404, and the services \ tcpip \ parameters \ terrange \ terr$ c7d49d7cecdc}[dhcpserver]

Queries value:

c7d49d7cecdc}[queryadaptername]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[disableadapterdomainname]

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4300-abe3-4300-a$ c7d49d7cecdc}[registrationenabled]

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-4404, and the services \ tcpip \ parameters \ terrange \ terr$ c7d49d7cecdc}[registeradaptername]

Queries value:

c7d49d7cecdc}[registrationmaxaddresscount]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[maxnumberofaddressestoregister]

Queries value:

c7d49d7cecdc}[domain]

Oueries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-4404, and the services \ tcpip \ parameters \ terrange \ terr$ c7d49d7cecdc}[dhcpdomain]

Queries value:

c7d49d7cecdc}[ipautoconfigurationenabled]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[addresstype] Oueries value:

c7d49d7cecdc}[nameserver]

Oueries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-4404, and the services \ tcpip \ parameters \ terrange \ terr$ c7d49d7cecdc}[dhcpnameserver]

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

Oueries value:

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

Queries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]

Oueries value: $HKLM \ software \ microsoft \ strong$ cryptographic provider[type]

HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong Oueries value: 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]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]

HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll] Oueries value: HKCU\appevents\schemes\apps\.default\systemnotification\.current[] Oueries value:

Oueries value: HKLM\software\microsoft\com3[regdbversion]

Queries value: HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}[appid] HKCR\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}[dllsurrogate] Oueries value: Queries value: $HKCR \land ppid \land \{27af75ed-20d9-11d1-b1ce-00805fc1270e\} [local service]$ Queries value: HKCR\clsid\{33c4643c-7811-46fa-a89a-

768597bd7223}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserver32[]

Queries value: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}[appid]

Queries value: HKCR\clsid\{2227a280-3aea-1069-a2de-

08002b30309d}\shellfolder[wantsfordisplay]

Queries value: HKCR\clsid\{2227a280-3aea-1069-a2de-

08002b30309d}\shellfolder[attributes]

Queries value: HKCR\clsid\{2227a280-3aea-1069-a2de-

08002b30309d}\shellfolder[callforattributes]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{2227a280-3aea-1069-a2de-1060-a2de-1060-a2de-1060-a2de$

08002b30309d}]

Queries value: HKCR\clsid\{2227a280-3aea-1069-a2de-

08002b30309d}\shellfolder[hidefolderverbs]

Queries value: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}[localizedstring]

 $HKCU\software\microsoft\windows\shellnoroam\muicache[@c:\windows\system32\shell32.dll,-9319]$

Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-

00805fc1270e}\shellfolder[wantsfordisplay]

Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-

00805fc1270e}\shellfolder[attributes]

Oueries value:

HKLM\software\microsoft\windows\currentversion\policies\nonenum[{7007acc7-3202-11d1-aad2-

00805fc1270e}]

Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-

00805fc1270e}\shellfolder[hidefolderverbs]

Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[localizedstring]

Queries value:

 $HKCU \ software \ microsoft \ windows \ shell no roam \ muicache [@c:\windows \ system 32 \ net shell. dll, -1200] \\$

Sets/Creates value: HKLM\software\microsoft\active setup\installed components\{9d71d88c-

c598-4935-c5d1-43aa4db90836}[stubpath]

Sets/Creates value: HKLM\software\bifrost[nck]
Sets/Creates value: HKCU\software\bifrost[klg]

Sets/Creates value:

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

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

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

folders[appdata]

Value changes: HKCU\sessioninformation[programcount]

Value changes: HKLM\software\microsoft\active setup\installed components\{9d71d88c-

c598-4935-c5d1-43aa4db90836}[stubpath]