Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3311, Task ID: 752

Task ID: 752 Risk Level: 10

Date Processed: 2016-05-18 10:34:07 (UTC)

Processing Time: 64.03 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\2a29e3a5d469fbc803a504464393f98e.exe"

Sample ID: 3311
Type: basic
Owner: admin

Label: 2a29e3a5d469fbc803a504464393f98e

Date Added: 2016-05-18 10:30:49 (UTC)
File Type: PE32:win32:gui

File Type: PE32:win32:gui File Size: 1127085 bytes

MD5: 2a29e3a5d469fbc803a504464393f98e

SHA256: c16b99b6dd2073d18c21dc2a0a24ba4b99355ab89405e9abf1d902d7f841f5cd

Description: None

Pattern Matching Results

10 Creates malicious mutex: DarkComet [APT, RAT]

Writes to memory of system processes

YARA score 7

7 Injects thread into Windows process

Creates threads in system processes

4 Connects to local IP

5 Possible injector

Static Events

YARA rule hit: KeyLoggerStrings

Anomaly: PE: Contains a virtual section

Process/Thread Events

Creates process: C:\WINDOWS\Temp\2a29e3a5d469fbc803a504464393f98e.exe

["c:\windows\temp\2a29e3a5d469fbc803a504464393f98e.exe"]

Creates process: C:\WINDOWS\system32\notepad.exe [notepad]
Writes to process: PID:348 C:\WINDOWS\system32\notepad.exe
Creates remote thread: C:\WINDOWS\system32\notepad.exe

Named Object Events

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

1957994488-1003

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

1957994488-1003

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

1957994488-1003

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

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

1957994488-1003 Creates mutex:

1957994488-1003

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

507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003

Creates mutex: \BaseNamedObjects\DC_MUTEX-F5B0MXB
Creates mutex: \BaseNamedObjects\SHIMLIB_LOG_MUTEX

Creates mutex: \BaseNamedObjects\DCPERSFWBP

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

 $\label{lem:continuous} Creates semaphore: $$ \aseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}$$ Creates semaphore: $$ \aseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}$$ Creates semaphore: $$ \aseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}$$$

File System Events

Creates: C:\Documents and Settings\Admin\Application Data\dclogs
Opens: C:\WINDOWS\Prefetch\2A29E3A5D469FBC803A504464393F-00D92855.pf

Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\system32\wsock32.dl1
Opens: C:\WINDOWS\system32\ws2_32.dl1
Opens: C:\WINDOWS\system32\ws2help.dl1
Opens: C:\WINDOWS\system32\winmm.dl1
Opens: C:\WINDOWS\system32\netapi32.dl1

C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-ww_dfb54e0c Opens:

C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-ww dfb54e0c\GdiPlus.dll

W_d1b54e0C\Gd1P1uS.d11

Opens: C:\WINDOWS\system32\msacm32.dll

```
C:\WINDOWS\system32\shfolder.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\avicap32.dll
 Opens:
                         C:\WINDOWS\system32\msvfw32.dll
                         C:\WINDOWS\Temp\2a29e3a5d469fbc803a504464393f98e.exe
 Opens:
 Opens:
                         C:\WINDOWS\svstem32\imm32.dll
 Opens:
                         C:\WINDOWS\system32\shell32.dll
                         C:\WINDOWS\system32\shell32.dll.124.Manifest
 Opens:
                         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
 Opens:
                         C:\WINDOWS\WindowsShell.Manifest
                         C:\WINDOWS\WindowsShell.Config
 Opens:
 Opens:
                         C:\windows\temp\2a29e3a5d469fbc803a504464393f98e.exe.124.Manifest
                         C:\WINDOWS\system32\URLMON.DLL.123.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\URLMON.DLL.123.Config
 Opens:
                         C:\WINDOWS\system32\comctl32.dll
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Config
 Opens:
                         C:\WINDOWS\system32\wininet.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\wininet.dll.123.Config
 Opens:
                         C:\WINDOWS\svstem32\MSCTF.dll
 Opens:
                         C:\WINDOWS\system32\MSCTFIME.IME
 Opens:
                         C:\WINDOWS\system32\rpcss.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\notepad.exe
 Opens:
                         C:\WINDOWS\system32\apphelp.dll
 Opens:
                         C:\WINDOWS\AppPatch\sysmain.sdb
 Opens:
                         C:\WINDOWS\AppPatch\systest.sdb
 Opens:
                         C:\WINDOWS\system32
 Opens:
                         C:\WINDOWS
 Opens:
                         C:\WINDOWS\system32\notepad.exe.Manifest
 Opens:
                         C:\WINDOWS\system32\notepad.exe.Config
 Opens:
                         C:\WINDOWS\Prefetch\NOTEPAD.EXE-336351A9.pf
 Opens:
                         C:\WINDOWS\system32\winspool.drv
 Opens:
                         C:\WINDOWS\system32\shimeng.dll
 Opens:
                         C:\WINDOWS\AppPatch\AcGenral.dll
 Opens:
                         C:\WINDOWS\system32\uxtheme.dll
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Config
 Opens:
 Opens:
                         C:\WINDOWS\AppPatch
                         C:\WINDOWS\WinSxS
 Opens:
 Opens:
                         C:\WINDOWS\system32\ntdll.dll
 Opens:
                         C:\WINDOWS\system32\kernel32.dll
 Opens:
                         C:\WINDOWS\system32\unicode.nls
 Opens:
                         C:\WINDOWS\system32\setupapi.dll
                         C:\WINDOWS\system32\locale.nls
 Opens:
 Opens:
                         C:\WINDOWS\system32\sorttbls.nls
 Opens:
                         C:\WINDOWS\system32\comdlg32.dll
 Opens:
                         C:\WINDOWS\system32\advapi32.dll
 Opens:
                         C:\WINDOWS\system32\rpcrt4.dll
 Opens:
                         C:\WINDOWS\system32\secur32.dll
 Opens:
                         C:\WINDOWS\system32\msvcrt.dll
 Opens:
                         C:\WINDOWS\system32\gdi32.dl1
 Opens:
                         C:\WINDOWS\system32\user32.dll
 Opens:
                         C:\WINDOWS\system32\shlwapi.dll
 Opens:
                         C:\WINDOWS\system32\ole32.dll
 Opens:
                         C:\WINDOWS\system32\oleaut32.dll
 Opens:
                         C:\WINDOWS\system32\version.dll
 Opens:
                         C:\WINDOWS\system32\userenv.dll
 Opens:
                         C:\WINDOWS\system32\ctype.nls
 Opens:
                         C:\WINDOWS\system32\sortkey.nls
                         C:\WINDOWS\system32\MSIMTF.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\narrhook.dll
 Opens:
                         C:\WINDOWS\system32\oleacc.dll
 Opens:
                         C:\WINDOWS\system32\msvcp60.dl1
 Opens:
                         C:\WINDOWS\system32\oleaccrc.dll
                         C:\Documents and Settings
 Opens:
                         C:\Documents and Settings\Admin\Application Data\desktop.ini
 Opens:
 Opens:
                         C:\WINDOWS\Fonts\lucon.ttf
 Opens:
                         C:\WINDOWS\system32\mswsock.dll
 Opens:
                         C:\WINDOWS\system32\hnetcfg.dll
 Opens:
                         C:\WINDOWS\system32\wshtcpip.dll
 Reads from:
                         C:\WINDOWS\Temp\2a29e3a5d469fbc803a504464393f98e.exe
 Reads from:
                         C:\WINDOWS\Prefetch\NOTEPAD.EXE-336351A9.pf
 Reads from:
                         C:\Documents and Settings\Admin\Application Data\desktop.ini
```

Network Events

Windows Registry Events

options\shfolder.dll

Creates key: HKCU\software\microsoft\windows\currentversion\internet settings Creates key: HKCU\software\microsoft\multimedia\audio Creates key: HKCU\software\microsoft\multimedia\audio compression manager\ Creates key: HKCU\software\microsoft\multimedia\audio compression manager\msacm HKCU\software\microsoft\multimedia\audio compression manager\priority Creates key: v4.00 Creates key: HKCU\software HKCU\software\dc3_fexec Creates kev: Creates key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders Creates key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders Creates key: 806d6172696f}\ Creates key: HKCU\software\microsoft\notepad Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\2a29e3a5d469fbc803a504464393f98e.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 HKCU\software\policies\microsoft\windows\safer\codeidentifiers Opens key: Opens kev: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots Opens key: $\label{lem:hklm} \mbox{HKLM} \mbox{$\tt M$} \mbox{$\tt M$}$ options\secur32.dll Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$ options\rpcrt4.dll Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution options\advapi32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\winlogon HKLM∖ Opens key: Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ diagnostics$ 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 kev: HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\gdi32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: 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 HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\ws2help.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ws2_32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wsock32.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: options\shlwapi.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shell32.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 key: options\urlmon.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\normaliz.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wininet.dll Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution options\winmm.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\netapi32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\gdiplus.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msacm32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvfw32.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\avicap32.dll Opens kev: HKLM\system\currentcontrolset\control\error message instrument\ Opens key: HKLM\system\currentcontrolset\control\error message instrument HKLM\software\microsoft\windows nt\currentversion\gre_initialize Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32 Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility HKLM\software\microsoft\windows nt\currentversion\windows Opens key: Opens key: HKLM\software\microsoft\ole Opens key: HKCR\interface Opens key: HKCR\interface\{00020400-0000-0000-c000-00000000046} HKLM\software\microsoft\oleaut Opens key: Opens key: HKLM\software\microsoft\oleaut\userera Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance HKLM\system\setup Opens kev: Opens key: HKCU\ Opens key: HKCU\software\policies\microsoft\control panel\desktop HKCU\control panel\desktop Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack HKCU\software\classes\ Opens kev: Opens key: HKCU\software\classes\protocols\name-space handler\ Opens key: HKCR\protocols\name-space handler HKCU\software\classes\protocols\name-space handler Opens key: Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings HKLM\software\microsoft\windows\currentversion\internet settings Opens key: Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_protocol_lockdown Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\ HKLM\software\policies\microsoft\internet explorer\main\featurecontrol Opens key: Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol Opens key: $\label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\mbox{\sc main\feature} control} \\$ Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\ Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}$ settings\zonemap\domains\ HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zonemap\ranges\ HKCU\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zonemap\ranges\ HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_unc_savedfilecheck Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck HKLM\system\currentcontrolset\control\wmi\security Opens key: HKLM\software\microsoft\windows nt\currentversion\drivers32 Opens key: Opens key: HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm Opens key: $HKLM \backslash software \backslash microsoft \backslash audio compression manager \backslash driver cache$ Opens key: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.ima adpcm$ $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msadpc manager \setminus driver cache \setminus msadpc manager \setminus driver cache \setminus msadpc msa$ Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711 Opens key: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. \ msgsm610$ $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. trspch$ Opens kev: Opens key: Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1 Opens key: Opens kev: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2 Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm Opens key: HKLM\system\currentcontrolset\control\mediaresources\acm Opens key: HKLM\software\microsoft\windows nt\currentversion\vfw

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\fontsubstitutes

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

options\msctf.dll

Opens key:

HKLM\software\microsoft\ctf\compatibility\2a29e3a5d469fbc803a504464393f98e.exe

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

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\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\hardware\devicemap\video

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

Opens key:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9$

Opens key:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus protocol_catalog 9 \setminus 00000004$

Opens key:

Opens key:

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

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

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \protocol_catalog 9 \catalog_entries \noon 000000000010 \parameters \end{subarray}.$ Opens key:

 $\label{lem:hklm} \begin{tabular}{ll} HKLM \system \current control set \services \winsock 2 \parameters \protocol_catalog 9 \catalog_entries \000000000011 \parameters \end{tabular}$ Opens key:

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog 5$

Opens key:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace_catalog 5 \setminus 00000004$

Opens key

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000001

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

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

Opens key: HKLM\software\microsoft\rpc

Opens key: $\qquad \qquad \text{HKLM} \\ \text{software} \\ \text{microsoft} \\ \text{windows nt} \\ \text{currentversion} \\ \text{image file execution}$

 $options \verb|\| 2a29e3a5d469fbc803a504464393f98e.exe \verb|\| rpcthreadpoolthrottle | and a superior of the contraction of the contr$

 $\label{lem:control} \mbox{ Opens key:} \qquad \mbox{ HKLM} \mbox{ htcmsoftware policies microsoft windows nt rpc } \\ \mbox{ Opens key:} \qquad \mbox{ HKLM} \mbox{ system current control set l computer name } \\ \mbox{ } \mbox{$

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

Opens key: $\label{lem:hklmsystem} \verb| HKLM | system | current control | idconfigdb | lem | control | lem | co$

Opens key: HKLM\system\currentcontrol\set\control\idconfigdb\hardware profiles\0001
Opens key: HKLM\system\currentcontrol\set\control\idconfigdb\currentdockinfo

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

Opens key: HKCU\software\dc3_fexec
Opens key: HKCU\software\dc2_users

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

options\apphelp.dll

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

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\notepad.exe

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\software\policies\microsoft\windows\safer\levelobjects

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

Opens key:

```
be2efd2c1a33}
                           HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
 Opens kev:
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}
 Opens key:
7c29ddecae3f}
 Opens key:
085bcc18a68d}
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
h91490411hfc3
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
 Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus paths
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
 Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus paths
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
 Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus hashes
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
 Opens key:
                           HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
                           HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
 Opens kev:
 Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus urlzones
 Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
 Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
 Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
 Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus paths
 Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
 Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
 Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
 Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
 Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
 Opens kev:
HKCU \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ \ 262144 \ paths
 Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
 Opens kev:
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\notepad.exe
 Opens key:
                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\acgenral.dll
 Opens key:
                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comdlg32.dll
 Opens key:
                           HKLM\software\microsoft\windows nt\currentversion\image file execution
```

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

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

options\winspool.drv
Opens key:

options\shimeng.dll
 Opens key:

options\userenv.dll

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

options\uxtheme.dll

 $\label{lem:constant} Opens~key: & HKLM\software\microsoft\windows\currentversion\policies\explorer \\ Opens~key: & HKCU\software\microsoft\windows\currentversion\policies\explorer \\ \end{tabular}$

Opens key:

 $HKLM\software\mbox{\tt hicrosoft\windows\currentversion\shell} compatibility\applications\2a29e3a5d469fbc803a504464393f98e. exercise the substitution of the substitut$

Opens key:

a2d8-08002b30309d}

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

08002b30309d}\inprocserver32

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

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

options\setupapi.dll

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

Opens key: HKLM\system\wpa\pnp

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

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

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

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

Opens key:

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{f90255c2-6bc4-f8025bc4-f8025bc2-6bc4-f8025bc2-6bc4-f8025bc2-6bc4-f8025bc2-6bc4-f802bc2-f802bc$

11e3-9fc7-806d6172696f}\

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

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

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

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

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

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

Opens key: HKCR\directory\clsid

Opens key: HKCU\software\classes\folder

Opens key: HKCR\folder

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

Opens key: HKCR\folder\clsid

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

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

folders

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

Opens key: HKCU\software\microsoft\windows\currentversion\thememanager
Opens key: HKLM\software\microsoft\ctf\compatibility\notepad.exe

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

options\mswsock.dll

 $Opens\ key: \\ HKLM\software\microsoft\windows\ nt\currentversion\sim ge \ file\ execution$

options\hnetcfg.dll

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

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

options\wshtcpip.dll

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

Queries value:

 $HKLM \verb|\software| policies \verb|\microsoft| windows \verb|\safer| code identifiers[transparentenabled]|$

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

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

nt\currentversion\compatibility32[2a29e3a5d469fbc803a504464393f98e]

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

compatibility[2a29e3a5d469fbc803a504464393f98e]

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

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

manager[criticalsectiontimeout]

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

Queries value: HKCR\interface[interfacehelperdisableal1]
Queries value: HKCR\interface[interfacehelperdisableal1forole32]
Queries value: HKCR\interface[interfacehelperdisabletypelib]
Queries value: HKCR\interface\{00020400-0000-0000-c000-

00000000046}[interfacehelperdisableall]

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

00000000046}[interfacehelperdisableallforole32]

 Queries value:
 HKLM\system\setup[systemsetupinprogress]

 Queries value:
 HKCU\control panel\desktop[multiuilanguageid]

 Queries value:
 HKCU\control panel\desktop[smoothscroll]

Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips] Oueries value: HKLM\software\microsoft\windows\currentversion\internet

settings[disableimprovedzonecheck]

HKLM\software\microsoft\internet Oueries value:

explorer\main\featurecontrol\feature_protocol_lockdown[2a29e3a5d469fbc803a504464393f98e.exe]

Oueries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[*]

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

ab78-1084642581fb]

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

0000-0000000000001

Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3] Oueries value:

Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]

HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3] Queries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]

Oueries value:

HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]

Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1] Oueries value: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ drivers 32 [mixer 2]$ 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] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6] Oueries 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]

Oueries value: HKCU\software\microsoft\multimedia\audio[svstemformats]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\drivers32[msacm.imaadpcm]

Oueries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[fdwsupport]

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags] Oueries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[aformattagcache] Oueries value:

 $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. im a adpcm [cfilter tags]$

HKLM\software\microsoft\windows

nt\currentversion\drivers32[msacm.msadpcm]

Queries value:

 $HKLM \label{lem:hklm} \\ HKLM \label{lem:hklm} HKLM \label{lem:hklm} \\ HKLM \label{lem:hkklm} \\ HKLM \label{$

Oueries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cformattags]

HKLM\software\microsoft\audiocompressionmanager\drivercache\msadpcm[aformattagcache] Queries value:

HKLM\software\microsoft\windows Oueries value:

nt\currentversion\drivers32[msacm.msg711]

Oueries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[fdwsupport]

Oueries value:

Oueries value:

 $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. msg 711 [a formattag cache]$

Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cfiltertags] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msgsm610] Oueries value: Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cformattags] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[aformattagcache] Oueries value: $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msgsm610 [cfilter tags]$ HKLM\software\microsoft\windows Oueries value: nt\currentversion\drivers32[msacm.trspch] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cformattags] Oueries value: Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cfiltertags] HKLM\software\microsoft\windows Oueries value: nt\currentversion\drivers32[msacm.msg723] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[fdwsupport] HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cformattags] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[aformattagcache] Oueries value: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. \\ msg723[cfilter tags]$ HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msaudio1] Oueries value: Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cformattags] Oueries value: $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msaudio1[cfilter tags]$ HKLM\software\microsoft\windows Oueries value: nt\currentversion\drivers32[msacm.sl_anet] $HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus msacm. sl_anet[fdwsupport]$ Oueries value: Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[aformattagcache] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl anet[cfiltertags] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cformattags] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[aformattagcache] HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cfiltertags] Oueries value: $\label{local-operator} \mbox{HKLM\software\mbox{\sc microsoft\windows} nt\current version\drivers 32[msacm.13acm]} \mbox{\sc microsoft\windows} \mbox{\sc micro$ HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.13acm[fdwsupport] Oueries value: $HKLM \verb|\software\microsoft\audiocompressionmanager\drivercache\mbox| 13acm[cformattags]$ Queries value: $HKLM \verb|\software\m| icrosoft\audiocompression manager\driver cache \verb|\m| sacm. 13acm [aformattag cache] \\$ Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags] Queries value: HKCU\software\microsoft\multimedia\audio compression manager\msacm[nopcmconverter] HKCU\software\microsoft\multimedia\audio compression manager\priority Oueries value: v4.00[priority1] Queries value: $\label{lem:hklm} \verb+Kklm \+ software \+ microsoft \+ windows nt \+ current version \+ fontsubstitutes [ms]$ shell dlg 21 Queries value: HKLM\software\microsoft\ctf\systemshared[cuas] Oueries value: HKCU\keyboard layout\toggle[language hotkey] HKCU\keyboard layout\toggle[hotkey] Oueries value:

HKCU\keyboard layout\toggle[layout hotkey]

HKLM\software\microsoft\ctf[enableanchorcontext]

HKLM\software\microsoft\windows nt\currentversion\imm[ime file]

HKCU\software\microsoft\ctf[disable thread input manager]

Oueries value:

Queries value:

Queries value: Queries value: Queries value: HKLM\hardware\devicemap\video[maxobjectnumber]
Queries value: HKLM\hardware\devicemap\video[\device\video0]

Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters [winsock_registry_version]$

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]

Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]

Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000002[packedcatalogitem]

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
Queries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ catalog_entries \ 0000000000008 \ [packed catalog item] \ Queries \ value:$

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries \ 0000000000009 \ [packed catalog item] \\ Queries \ value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
 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]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring]
Oueries 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\000000000001[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] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
Oueries 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]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[storesserviceclassinfo]
 Oueries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
Oueries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[addressfamily]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 0000000000003 \ [enabled] \ Oueries \ value:$

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \namespace_catal$

```
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog\_entries \ (00000000003[storesserviceclass info]) \ (catalog\_entries) \ 
     Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
                                                                            HKLM\software\microsoft\rpc[maxrpcsize]
     Queries value:
     Queries value:
HKLM\system\currentcontrolset\computername\activecomputername[computername]
                                                                            HKLM\system\currentcontrolset\control\idconfigdb[currentconfig]
     Queries value:
     Queries value:
HKLM\system\currentcontrolset\control\idconfigdb\currentdockinfo[dockingstate]
                                                                            HKLM \setminus system \setminus current control \setminus idconfigdb \setminus hardware
     Queries value:
profiles\0001[dockstate]
                                                                            {\tt HKLM \ } system \verb|\ current control \verb|\ idconfigdb \verb|\ hardware \\
     Queries value:
profiles\0001[hwprofileguid]
     Queries value:
                                                                            HKLM\system\currentcontrolset\control\idconfigdb\hardware
profiles\0001[friendlyname]
                                                                            HKLM\software\microsoft\windows\currentversion[programfilesdir]
     Queries value:
                                                                             HKLM\system\currentcontrolset\control\session
     Queries value:
manager[safeprocesssearchmode]
                                                                             HKLM\system\currentcontrolset\control\session
     Queries value:
manager\appcompatibility[disableappcompat]
                                                                            HKLM\system\wpa\mediacenter[installed]
     Oueries value:
     Queries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [authenticode enabled]
     Queries value:
                                                                           HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
     Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}[itemdata]
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ paths \ \{dda3f824-d8cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-834d-48cb-441b-836d-48cb-441b-836d-48cb-441b-836d-48cb-441b-836d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d-48cb-460d
be2efd2c1a33}[saferflags]
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemdata]
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[hashalg]
     Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemsize]
     Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[saferflags]
     Oueries value:
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{7fb9cd2e-3076-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57
b813f72dbb91}[itemdata]
     Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[hashalg]
     Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[itemsize]
     Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[saferflags]
     Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemdata]
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[hashalg]
```

Queries value:

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

Queries value

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

Queries value:

 $\label{lem:hklmsoftware} HKLM\software \policies \microsoft\windows \safer\code identifiers \oldsymbol{lem:hklmsoftware} \part \pa$

Queries value:

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

Queries value:

 $HKLM \software \policies \microsoft \windows \safer \code identifiers \noindent \noi$

Queries value:

Queries value:

Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2eb91490411bfc}[hashalg] Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2eb91490411bfc}[itemsize] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2eb91490411bfc}[saferflags] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel] Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cache] Queries value:

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

Queries value: HKLM\software\microsoft\windows

nt\currentversion\compatibility32[notepad]

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

compatibility[notepad]

Queries value: HKCU\software\dc3_fexec[{5f6daf40-6bc5-11e3-ae04-806d6172696f-

2094477158}1

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

folders[appdata] Queries value:

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

Queries value:

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

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

Queries value:

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

Queries value:

 $HKCU \ software \ \verb|microsoft| windows \ \verb|currentversion| policies \ \verb|explorer[nocontrol panel]| \\$

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

HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[] Oueries value:

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

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

Oueries value:

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

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

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

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

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

Queries value:

 $HKCU \ software \ microsoft \ windows \ current version \ \ explorer \ mountpoints 2 \ cpc \ \ \ \{f90255c2-6bc4-f90256c2-6bc4-f90256c4-f90256c4-f90256c4-f90256c4-f90256c4-f90256c4-f90256c4-f90256c4-f90256c4-f90256c4-f9026c4-f90256c4-f90256c4-f9026c4-f90256c4-f9026c4-f$

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

Oueries value:

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

Queries value:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [forceactive desktop on] \\$

Oueries value:

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

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

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

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

 $\label{thm:linear} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\policies\explorer[nonetcrawling]}}$

Queries value:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \current version \explorer \advanced [hidden] \end{tabular}$ Oueries value:

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

```
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
                                     HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
  Oueries value:
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
  Queries value:
                                     HKCR\directory[docobject]
  Queries value:
                                      HKCR\directory[browseinplace]
                                     HKI M\software\microsoft\windows
  Oueries value:
nt\currentversion\winlogon[userenvdebuglevel]
  Queries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\winlogon[chkaccdebuglevel]
  Queries value:
                                     HKCR\directory[isshortcut]
  Queries value:
                                      HKCR\directory[alwaysshowext]
  Oueries value:
                                     HKCR\directorv[nevershowext]
  Queries value:
                                      HKLM\system\currentcontrolset\control\productoptions[producttype]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
                                      HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Queries value:
folders[personal]
                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Oueries value:
folders[local settings]
  Queries value:
                                      HKLM\software\microsoft\windows
nt\currentversion\winlogon[rsopdebuglevel]
                                      HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
  Queries value:
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
                                      HKCU\control panel\desktop[lamebuttontext]
  Oueries value:
  Queries value:
                                      HKCU\software\microsoft\notepad[lfescapement]
  Queries value:
                                      HKCU\software\microsoft\notepad[lforientation]
  Oueries value:
                                      HKCU\software\microsoft\notepad[lfweight]
                                      HKCU\software\microsoft\notepad[lfitalic]
  Queries value:
  Queries value:
                                      HKCU\software\microsoft\notepad[lfunderline]
  Oueries value:
                                      HKCU\software\microsoft\notepad[lfstrikeout]
  Queries value:
                                      HKCU\software\microsoft\notepad[lfcharset]
  Queries value:
                                      HKCU\software\microsoft\notepad[lfoutprecision]
  Oueries value:
                                      HKCU\software\microsoft\notepad[lfclipprecision]
                                      HKCU\software\microsoft\notepad[lfquality]
  Oueries value:
  Queries value:
                                      HKCU\software\microsoft\notepad[lfpitchandfamily]
  Oueries value:
                                      HKCU\software\microsoft\notepad[lffacename]
  Queries value:
                                      HKCU\software\microsoft\notepad[ipointsize]
  Oueries value:
                                      HKCU\software\microsoft\notepad[fwrap]
  Oueries value:
                                      HKCU\software\microsoft\notepad[statusbar]
                                      HKCU\software\microsoft\notepad[fsavewindowpositions]
  Oueries value:
                                      HKCU\software\microsoft\notepad[szheader]
  Oueries value:
  Queries value:
                                      HKCU\software\microsoft\notepad[sztrailer]
                                      HKCU\software\microsoft\notepad[imargintop]
  Queries value:
  Oueries value:
                                      HKCU\software\microsoft\notepad[imarginbottom]
  Queries value:
                                      HKCU\software\microsoft\notepad[imarginleft]
                                      HKCU\software\microsoft\notepad[imarginright]
  Oueries value:
                                      HKCU\software\microsoft\notepad[iwindowposy]
  Oueries value:
  Oueries value:
                                      HKCU\software\microsoft\notepad[iwindowposx]
                                      HKCU\software\microsoft\notepad[iwindowposdx]
  Queries value:
  Queries value:
                                      HKCU\software\microsoft\notepad[iwindowposdy]
  Oueries value:
                                      HKCU\software\microsoft\notepad[fmle_is_broken]
                                      HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
  Queries value:
  Queries value:
                                      HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Oueries value:
                                      HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
HKLM\svstem\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
  Value changes:
                                     HKLM\software\microsoft\cryptography\rng[seed]
  Value changes:
                                      HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[appdata]
  Value changes:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints 2 \ \{f90255c2-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7-6bc4-11e3-9fc7
```

806d6172696f}[baseclass]