Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 630, Task ID: 2466

Task ID: 2466 Risk Level: 10

Date Processed: 2016-02-22 05:33:05 (UTC)

Processing Time: 61.22 seconds IntelliVM Virtual Environment:

Execution Arguments:

c:\windows\temp\d269f3af57167a25a289bc6fd3375c3f03d79044d9569e1de63a90c70fb7be33.exe"

Sample ID: 630 basic Type: admin Owner:

d269f3af57167a25a289bc6fd3375c3f03d79044d9569e1de63a90c70fb7be33 Label:

2016-02-22 05:26:50 (UTC) Date Added:

File Type: PE32:win32:gui File Size: 29616 bytes

6a2ea24ed959ef96d270af5cdc2f70a7 MD5:

SHA256: d269f3af57167a25a289bc6fd3375c3f03d79044d9569e1de63a90c70fb7be33

Description:

Pattern Matching Results

5 Creates process in suspicious location

5 Modifies Windows Registry from the command line

6 Modifies registry autorun entries

2 PE: Nonstandard section

8 Creates Suspicious Events: Localhost Ping

5 Adds autostart object

6 PE: Jumps to the last section near the entrypoint

4 Terminates process under Windows subfolder

10 YARA score 10

Static Events

YARA rule hit:	Hurix
Anomaly:	PE: No DOS stub
Anomaly:	PE: Contains one or more non-standard sections
Anomaly:	PE: Jumps to the last section near the entrypoint

Process/Thread Events

Creates process:

C:\WINDOWS\Temp\d269f3af57167a25a289bc6fd3375c3f03d79044d9569e1de63a90c70fb7be33.exe ["c:\windows\temp\d269f3af57167a25a289bc6fd3375c3f03d79044d9569e1de63a90c70fb7be33.exe"]

Creates process: C:\WINDOWS\system32\cmd.exe [cmd.exe /c reg add

HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v "CitrixXenAppReciever" /t REG_SZ /d

"C:\Documents and Settings\All Users\CitrixReciever\CitrixReciever.exe"]

Creates process: C:\WINDOWS\system32\cmd.exe [cmd.exe /c cmd.exe /c cmd.exe /c cmd.exe /c cmd.exe /c cmd.exe /c "C:\Documents and Settings\All Users\CitrixReciever\CitrixReciever.exe"]

C:\WINDOWS\system32\cmd.exe [cmd.exe /c ping 127.0.0.1 & del Creates process: c:\windows\temp\d269f3af57167a25a289bc6fd3375c3f03d79044d9569e1de63a90c70fb7be33.exe"]

C:\WINDOWS\system32\reg.exe [reg add

HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v "CitrixXenAppReciever" /t REG_SZ /d

"C:\Documents and Settings\All Users\CitrixReciever\CitrixReciever.exe"]

C:\WINDOWS\system32\cmd.exe [cmd.exe /c cmd.exe /c cmd.exe /c cmd.exe /c

cmd.exe /c "C:\Documents and Settings\All Users\CitrixReciever\CitrixReciever.exe"]

Creates process: C:\WINDOWS\system32\cmd.exe [cmd.exe /c cmd.exe /c cmd.exe /c cmd.exe /c

"C:\Documents and Settings\All Users\CitrixReciever\CitrixReciever.exe"] Creates process: C:\WINDOWS\system32\ping.exe [ping 127.0.0.1]

Creates process: C:\WINDOWS\system32\cmd.exe [cmd.exe /c cmd.exe /c cmd.exe /c

"C:\Documents and Settings\All Users\CitrixReciever\CitrixReciever.exe"]

C:\WINDOWS\system32\cmd.exe [cmd.exe /c cmd.exe /c "C:\Documents and Creates process: Settings\All Users\CitrixReciever\CitrixReciever.exe"]

C:\WINDOWS\system32\cmd.exe [cmd.exe /c "C:\Documents and Settings\All Creates process: Users\CitrixReciever\CitrixReciever.exe"]

Creates process: C:\Documents and Settings\All Users\CitrixReciever\CitrixReciever.exe ["C:\Documents and Settings\All Users\CitrixReciever\CitrixReciever.exe"]

Terminates process:

C:\WINDOWS\Temp\d269f3af57167a25a289bc6fd3375c3f03d79044d9569e1de63a90c70fb7be33.exe

Terminates process: C:\WINDOWS\system32\reg.exe Terminates process: C:\WINDOWS\system32\cmd.exe Terminates process: C:\WINDOWS\system32\ping.exe

Named Object Events

\BaseNamedObjects\SHIMLIB_LOG_MUTEX Creates mutex:

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

\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1} Creates semaphore:

File System Events

```
C:\Documents and Settings\All Users\CitrixReciever
 Creates
 Creates:
                         C:\Documents and Settings\All Users\CitrixReciever\CitrixReciever.exe
 Opens:
                         C:\WINDOWS\Prefetch\D269F3AF57167A25A289BC6FD3375-040BAF42.pf
 Opens:
                         C:\Documents and Settings\Admin
                         {\tt C:\WINDOWS\system32\imm32.dll}
 Opens:
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Config
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
 Opens:
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
 Opens:
                         C:\WINDOWS\WindowsShell.Manifest
 Opens:
                         C:\WINDOWS\WindowsShell.Config
 Opens:
                         C:\WINDOWS\system32\WININET.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\WININET.dll.123.Config
 Opens:
                         C:\WINDOWS\system32\shell32.dll
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Config
 Opens:
                         C:\WINDOWS\system32\comctl32.dll
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Config
 Opens:
                         C:\
                         C:\Documents and Settings\All Users\CitrixReciever\CitrixReciever.exe
 Opens:
 Opens:
C:\WINDOWS\Temp\d269f3af57167a25a289bc6fd3375c3f03d79044d9569e1de63a90c70fb7be33.exe
 Opens:
                         C:\Documents and Settings\All Users\CitrixReciever
 Opens:
                         C:\WINDOWS\system32\cmd.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\cmd.exe.Manifest
 Opens:
                         C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf
 Opens:
 Opens:
                         C:\WINDOWS\AppPatch
 Opens:
                         C:\WINDOWS\system32\wbem
 Opens:
                         C:\WINDOWS\WinSxS
 Opens:
                         C:\WINDOWS\system32\ntdll.dll
 Opens:
                         C:\WINDOWS\system32\kernel32.dll
 Opens:
                         C:\WINDOWS\system32\unicode.nls
 Opens:
                         C:\WINDOWS\system32\locale.nls
                         C:\WINDOWS\system32\sorttbls.nls
 Opens:
 Opens:
                         C:\WINDOWS\system32\msvcrt.dll
                         C:\WINDOWS\system32\user32.dll
 Opens:
                         C:\WINDOWS\system32\gdi32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\shimeng.dll
 Opens:
                         C:\WINDOWS\AppPatch\AcGenral.dll
 Opens:
                         C:\WINDOWS\system32\advapi32.dll
 Opens:
                         C:\WINDOWS\system32\rpcrt4.dll
 Opens:
                         C:\WINDOWS\system32\secur32.dll
 Opens:
                         C:\WINDOWS\system32\winmm.dll
 Opens:
                         C:\WINDOWS\system32\ole32.dll
 Opens:
                         C:\WINDOWS\system32\oleaut32.dll
 Opens:
                         C:\WINDOWS\system32\msacm32.dll
 Opens:
                         C:\WINDOWS\system32\version.dll
 Opens:
                         C:\WINDOWS\system32\shlwapi.dll
 Opens:
                         C:\WINDOWS\system32\userenv.dll
 Opens:
                         C:\WINDOWS\system32\uxtheme.dll
 Opens:
                         C:\WINDOWS\system32\ctype.nls
                         C:\WINDOWS\system32\sortkey.nls
 Opens:
 Opens:
                         C:\WINDOWS\system32\wbem\wmic.exe
 Opens:
                         C:\Documents and Settings
 Opens:
                         C:\WINDOWS\system32\reg.exe
 Opens:
                         C:\WINDOWS\system32\reg.exe.Manifest
 Opens:
                         C:\WINDOWS\Prefetch\REG.EXE-0D2A95F7.pf
 Opens:
                         C:\WINDOWS\system32\ping.exe
 Opens:
                         C:\WINDOWS\system32\ping.exe.Manifest
 Opens:
                         C:\WINDOWS\Prefetch\PING.EXE-31216D26.pf
                         C:\WINDOWS\system32\iphlpapi.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\ws2_32.dll
 Opens:
                         C:\WINDOWS\system32\ws2help.dll
 Opens:
                         C:\WINDOWS\system32\mswsock.dll
 Opens:
                         C:\WINDOWS\system32\hnetcfg.dll
 Opens:
                         C:\WINDOWS\system32\wshtcpip.dll
                         C:\Documents and Settings\All
 Opens:
Users\CitrixReciever\CitrixReciever.exe.Manifest
                         C:\WINDOWS\Prefetch\CITRIXRECIEVER.EXE-0C5B647C.pf
 Opens:
 Opens:
                         C:\WINDOWS\Temp
 Opens:
                         C:\WINDOWS\Temp\2bff810e-5143-453e-af20-4c0a7164214c
```

Writes to: C:\Documents and Settings\All Users\CitrixReciever\CitrixReciever.exe Reads from:

C:\WINDOWS\Temp\d269f3af57167a25a289bc6fd3375c3f03d79044d9569e1de63a90c70fb7be33.exe

Reads from: C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf

Deletes:

C:\WINDOWS\Temp\d269f3af57167a25a289bc6fd3375c3f03d79044d9569e1de63a90c70fb7be33.exe

Windows Registry Events

HKCU\software\microsoft\windows\currentversion\internet settings Creates key: HKCU\software\microsoft\multimedia\audio Creates key: Creates key: HKCU\software\microsoft\multimedia\audio compression manager\ Creates key: HKCU\software\microsoft\multimedia\audio compression manager\msacm Creates key: HKCU\software\microsoft\multimedia\audio compression manager\priority v4.00 Creates key: HKLM\software\microsoft\windows\currentversion\run Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\d269f3af57167a25a289bc6fd3375c3f03d79044d9569e1de63a90c70fb7be33.exe HKLM\svstem\currentcontrolset\control\terminal server Opens kev: 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 HKLM\system\currentcontrolset\control\safeboot\option Opens key: Opens key: $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers$ Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers 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\msvcrt.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\secur32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rpcrt4.dll $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ Opens key: options\advapi32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shlwapi.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\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\iertutil.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\urlmon.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wininet.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shell32.dll Opens kev: HKLM\svstem\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: $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus compatibility 32$ 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: Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics HKLM\software\microsoft\windows\currentversion\explorer\performance Opens key: Opens key: HKLM\software\microsoft\ole Opens key: HKCR\interface HKCR\interface\{00020400-0000-0000-c000-00000000046} Opens key: HKLM\software\microsoft\oleaut Opens key: Opens key: HKLM\software\microsoft\oleaut\userera Opens key: HKCU\ HKCU\software\policies\microsoft\control panel\desktop Opens key: Opens key: HKCU\control panel\desktop Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comctl32.dll $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\advanced}} \\$ Opens key:

 $\label{lem:hklm} \verb+KLM\+ software \verb+\microsoft\+ windows nt\+ current version \verb+\language pack+ \\$

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

HKCU\software\classes\

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

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

settings

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

settings

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

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

settings\

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

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

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

settings\zonemap\domains\

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

settings\zonemap\ranges\

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

settings\zonemap\ranges\

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

Opens key: HKLM\system\currentcontrolset\control\wmi\security

Opens key: HKLM\system\setup

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

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

options\apphelp.dll

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

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

HKLM\software\microsoft\windows Opens kev:

nt\currentversion\appcompatflags\custom\cmd.exe

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

options\version.dll

Opens kev: 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}

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

Opens kev:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{349d35ab-37b5-462f-9b89-4666f-9b89-46666$ edd5fbde1328}

Opens key:

b813f72dbb91}

Opens key:

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

085bcc18a68d}

Opens key:

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

Opens kev:

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

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus paths$

Opens kev:

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

Opens kev:

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

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths

Opens kev:

 $HKLM \ software \ \verb|\policies| microsoft| windows \ safer \ code identifiers \ \verb|\final of the code identifiers| as he will be a substitution of the code identifiers \ be a substitution of the cod$

```
Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus urlzones
      Opens kev:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
     Opens kev:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus hashes
     Opens key:
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
     Opens kev:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus hashes
     Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus urlzones
      Opens key:
                                                                                       HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
                                                                                       HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
      Opens key:
      Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
     Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus 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:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \end{tabular} $$ $$ \align{tabular}{ll} Akcular \end{tabular} $$ \align{tabular}{ll} Akcular
      Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
      Opens kev:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus urlzones
     Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
      Opens key:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \park \park
     Opens kev:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus paths
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\cmd.exe
     Opens key:
                                                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\acgenral.dll
      Opens key:
                                                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shimeng.dll
     Opens key:
                                                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\winmm.dll
     Opens key:
                                                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msacm32.dll
      Opens key:
                                                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\userenv.dll
     Opens key:
                                                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
                                                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32
      Opens key:
      Opens key:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
      Opens key:
                                                                                       HKLM \verb|\software\m| icrosoft \verb|\audiocompression manager\m| driver cache
      Opens key:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. imaadpcm \setminus driver cache \setminus driver ca
      Opens kev:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. msadpcm
```

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711

Opens key:

 $HKLM \verb|\software\m| icrosoft\audiocompression manager\driver cache \verb|\m| sacm. msgsm610$

Opens key: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. \ trspch$ HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723 Opens kev:

Opens key:

 $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. \ msaudio 1$ Opens key:

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

Opens key: $HKLM \verb|\software\microsoft\audiocompression manager\driver cache \verb|\msacm.iac2| \\$ Opens kev: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm

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

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

folders

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

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

Opens key: HKCU\software\policies\microsoft\windows\system Opens key: HKLM\software\microsoft\command processor Opens key: HKCU\software\microsoft\command processor

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

Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts

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

Opens key: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags\custom\reg.exe

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

options\reg.exe

Opens key: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags\custom\ping.exe

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

options\ping.exe

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\iphlpapi.dll

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

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

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

Opens key:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004 Opens kev:

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

Opens kev:

Opens kev:

Opens key:

Opens key:

Opens kev:

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

Opens key: Opens kev:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000011 Opens key:

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

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004

Opens kev:

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

Opens key:

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

Opens key:

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

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

options\mswsock.dll

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

options\hnetcfg.dll

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

Opens key: HKLM\software\microsoft\rpc

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

options\ping.exe\rpcthreadpoolthrottle

Opens key: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKLM\software\microsoft\rpc\securityservice

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

options\wshtcpip.dll

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

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

options\citrixreciever.exe

Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat] HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Oueries value:

Oueries value:

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

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

 $nt \verb|currentversion| compatibility 32[d269f3af57167a25a289bc6fd3375c3f03d79044d9569e1de63a90c70fb7be33]| to the following the$

Oueries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[d269f3af57167a25a289bc6fd3375c3f03d79044d9569e1de63a90c70fb7be33]

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

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

manager[criticalsectiontimeout]

Queries value: HKLM\software\microsoft\ole[rwlockresourcetimeout] Oueries value: HKCR\interface[interfacehelperdisableall]

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

00000000046}[interfacehelperdisableall]

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

00000000046}[interfacehelperdisableallforole32]

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

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus advanced [enable balloon tips]$

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

settings[disableimprovedzonecheck]

HKLM\software\microsoft\internet Queries value:

explorer\main\featurecontrol\feature_protocol_lockdown[d269f3af57167a25a289bc6fd3375c3f03d79044d9569e1de63a90c70fb7be33.exe]

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

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

ab78-1084642581fb]

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

0000-000000000000000

Oueries value: HKLM\system\setup[systemsetupinprogress]

Queries value:

HKLM\system\currentcontrolset\control\computername\activecomputername[computername]

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

manager[safeprocesssearchmode]

HKLM\svstem\currentcontrolset\control\session Oueries value:

manager\appcompatibility[disableappcompat]

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

Queries value:

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

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

be2efd2c1a33}[itemdata] Oueries value:

be2efd2c1a33}[saferflags]

Oueries value:

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

edd5fbde1328}[itemdata]

Oueries value:

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]

Oueries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{349d35ab-37b5-462f-9b89-4666f-9b89-46666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b$

edd5fbde1328}[saferflags]

Queries value:

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

b813f72dbb91}[itemdata]

Oueries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ has hes \ \{7fb9cd2e-3076-4df9-a57b-4df9-a5$ b813f72dbb91}[hashalg]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-

b813f72dbb91}[itemsize] Oueries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ has hes \ \{7fb9cd2e-3076-4df9-a57b-4df9-a5$

b813f72dbb91}[saferflags]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-

7c29ddecae3f}[itemdata]

Oueries value:

```
7c29ddecae3f}[hashalg]
    Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemsize]
    Oueries value:
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 10 \ hashes \ \{81d1fe15-dd9d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b1
7c29ddecae3f}[saferflags]
    Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemdata]
    Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[hashalg]
    Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemsize]
    Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[saferflags]
    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-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe
b91490411bfc}[itemdata]
    Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[hashalg]
    Queries value:
b91490411bfc}[itemsize]
    Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[saferflags]
    Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
    Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
                                                         HKCU\software\microsoft\windows\currentversion\explorer\shell
    Queries value:
folders[cache]
    Queries value:
\label{thm:loss} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} policies \end{tabular} irror soft \end{tabular} windows \end{tabular} software \end{tabular} policies \end{tabular} irror soft \end{tabular} windows \end{tabular} software \end{tabular} policies \end{tabular} method in \end{tabular} software \end{tabular} software \end{tabular} policies \end{tabular} windows \end{tabular} software \end{tabular} software
                                                         HKLM\software\microsoft\windows nt\currentversion\compatibility32[cmd]
    Queries value:
    Oueries value:
                                                          \label{lem:hklmsoftware} \verb+microsoft+ windows nt+ current version+ ime compatibility[cmd]
    Queries value:
                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
    Oueries value:
                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
    Oueries value:
                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
    Oueries value:
    Queries value:
                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
    Oueries value:
                                                          HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 5]
    Queries 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]
    Oueries value:
                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midil
    Queries value:
                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
    Queries value:
                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
    Oueries value:
                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
    Queries value:
                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
    Oueries value:
                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
    Oueries value:
                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi61]
    Oueries value:
                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
    Queries value:
    Queries value:
                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
    Oueries value:
                                                          HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [aux]
                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
    Queries value:
    Oueries value:
                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
    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]
    Queries value:
                                                          \label{lem:hklm} \mbox{ HKLM\software\mbox{\sc microsoft\windows nt\currentversion\drivers} aux 6] $$
    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]
    Queries value:
                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
    Queries value:
                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
    Oueries value:
                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
    Queries value:
                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
```

Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
Queries 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[mixer7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]

Queries value: HKCU\software\microsoft\multimedia\audio[systemformats]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\drivers32[msacm.imaadpcm]

Queries value:

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

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

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

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

Queries value: HKLM\software\microsoft\windows

nt\currentversion\drivers32[msacm.msadpcm]

Queries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[fdwsupport]
Oueries value:

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

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

Queries value: HKLM\software\microsoft\windows

nt\currentversion\drivers32[msacm.msg711]

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \audiocompression manager \driver cache \mbox{\sc msg711} [cformattags] \\ Queries value:$

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

 $HKLM \backslash software \backslash microsoft \backslash audio compression manager \backslash driver cache \backslash msacm. msg711[cfilter tags]$

Queries value: HKLM\software\microsoft\windows

nt\currentversion\drivers32[msacm.msgsm610]

Queries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[fdwsupport]

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cformattags]
Oueries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[aformattagcache]
 Oueries value:

 $HKLM \backslash software \backslash microsoft \backslash audio compression manager \backslash driver cache \backslash msacm. msgsm610 [cfilter tags]$

Queries value: HKLM\software\microsoft\windows

nt\currentversion\drivers32[msacm.trspch]

Queries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport]
 Oueries value:

 $\label{lem:hklm} HKLM \ software \ `microsoft\ `audiocompression manager\ 'driver cache \ `msacm.trspch[cformattags] \\ Oueries \ value:$

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

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cfiltertags]
Oueries value: HKLM\software\microsoft\windows

nt\currentversion\drivers32[msacm.msg723]

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft \audio compression manager \driver cache \mbox{\tt msg723[fdwsupport]} \\ Oueries \ value:$

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cformattags]
 Oueries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[aformattagcache]

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cfiltertags]
Queries value: HKLM\software\microsoft\windows

nt\currentversion\drivers32[msacm.msaudio1]

Oueries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[fdwsupport]
Queries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cformattags]
Queries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[aformattagcache]
Oueries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cfiltertags]
Queries value: HKLM\software\microsoft\windows

nt\currentversion\drivers32[msacm.sl_anet]

Queries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[fdwsupport]
 Oueries value:

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

 $\label{lem:hklmsoftware} HKLM\software\microsoft\audiocompression manager\drivercache\mbox{\sc m.sl_anet[aformattagcache]} \\ Queries\ value:$

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

Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2]

Queries value:

```
HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus msacm.iac2[fdwsupport]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cformattags]
 Queries value:
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. iac 2 [a formattag cache]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cfiltertags]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.13acm]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[fdwsupport]
 Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cformattags]
 Oueries value:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. 13 acm [a formattag cache]
 Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags]
                         HKCU\software\microsoft\multimedia\audio compression
 Oueries value:
manager\msacm[nopcmconverter]
                         HKCU\software\microsoft\multimedia\audio compression manager\priority
 Queries value:
v4.00[priority1]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\winlogon[userenvdebuglevel]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\winlogon[chkaccdebuglevel]
                         HKLM\system\currentcontrolset\control\productoptions[producttype]
 Queries value:
 Queries value:
                         \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}
folders[personal]
                         HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Queries value:
folders[local settings]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\winlogon[rsopdebuglevel]
                         HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
 Queries value:
 Queries value:
                         HKCU\control panel\desktop[lamebuttontext]
 Oueries value:
                         HKLM\software\microsoft\command processor[disableunccheck]
                         HKLM\software\microsoft\command processor[enableextensions]
 Queries value:
                         HKLM\software\microsoft\command processor[delayedexpansion]
 Oueries value:
 Oueries value:
                         HKLM\software\microsoft\command processor[defaultcolor]
                         HKLM\software\microsoft\command processor[completionchar]
 Queries value:
                         HKLM\software\microsoft\command processor[pathcompletionchar]
 Queries value:
 Oueries value:
                         HKLM\software\microsoft\command processor[autorun]
                         HKCU\software\microsoft\command processor[disableunccheck]
 Queries value:
 Oueries value:
                         HKCU\software\microsoft\command processor[enableextensions]
 Oueries value:
                         HKCU\software\microsoft\command processor[delayedexpansion]
 Oueries value:
                         HKCU\software\microsoft\command processor[defaultcolor]
                         HKCU\software\microsoft\command processor[completionchar]
 Queries value:
 Oueries value:
                         HKCU\software\microsoft\command processor[pathcompletionchar]
 Queries value:
                         HKCU\software\microsoft\command processor[autorun]
 Oueries value:
                         HKLM\svstem\currentcontrolset\control\nls\locale[00000409]
 Queries value:
                         HKLM\system\currentcontrolset\control\nls\language groups[1]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\compatibility32[reg]
                         HKLM\software\microsoft\windows nt\currentversion\ime compatibility[reg]
 Oueries value:
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\run[citrixxenappreciever]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\compatibility32[ping]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[ping]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
 Queries value:
Queries 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:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000003[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000006[packedcatalogitem]
```

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[packedcatalogitem]

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ 0000000000008 \ [packed catalog item]$

Queries value:

Oueries value:

Queries value:

Queries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]

Oueries value:

HKLM\system\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\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] Oueries value:

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]
 Oueries 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]
 Oueries value:

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

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

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

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
Queries value:

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultttl]

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

Queries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]

Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [minsock addrlength]$

Queries value:

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

Queries value:

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

 $\label{lem:hklm} \verb|HKLM| system| current control set| services \verb|\tcpip| parameters| winsock[helperdllname] \\$

Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[citrixreciever]

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

compatibility[citrixreciever]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_protocol_lockdown[citrixreciever.exe]

Sets/Creates value: HKLM\software\microsoft\windows\currentversion\run[citrixxenappreciever]

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