# Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3321, Task ID: 792

Task ID: 792 Risk Level: 10

Date Processed: 2016-05-18 10:38:46 (UTC)

Processing Time: 62.56 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\543bd82ec71ae746e83c14eba28494df.exe"

Sample ID: 3321 Type: basic Owner: admin

Label: 543bd82ec71ae746e83c14eba28494df

Date Added: 2016-05-18 10:30:50 (UTC)
File Type: PF32:win32:gui

File Type: PE32:win32:gui File Size: 147968 bytes

MD5: 543bd82ec71ae746e83c14eba28494df

SHA256: b5835739dfcf21ab4869dea949ccc6038ea65be94f11307154e2c58a404b53ec

Description: None

### Pattern Matching Results

6 Modifies registry autorun entries

- 5 Abnormal sleep detected
- 4 Checks whether debugger is present
- 10 Creates malicious events: Clisbot [Worm]
- 7 Changes DNS name server
- 4 Terminates process under Windows subfolder
- 5 PE: Contains compressed section
- 5 Adds autostart object
- 5 Installs service

## Process/Thread Events

Creates process: C:\WINDOWS\Temp\543bd82ec71ae746e83c14eba28494df.exe

["c:\windows\temp\543bd82ec71ae746e83c14eba28494df.exe" ]

Creates process: C:\WINDOWS\regedit.exe [regedit.exe /s

C:\DOCUME~1\Admin\LOCALS~1\Temp\rtf1.tmp]

Writes to process: PID:308 C:\WINDOWS\Temp\543bd82ec71ae746e83c14eba28494df.exe

Terminates process: C:\WINDOWS\Temp\543bd82ec71ae746e83c14eba28494df.exe

Terminates process: C:\WINDOWS\regedit.exe

## Named Object Events

Creates mutex: \BaseNamedObjects\1-4B4F4E4E494348492D5741-1

Creates mutex: \BaseNamedObjects\SHIMLIB\_LOG\_MUTEX

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

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

## File System Events

Creates: C:\Documents and Settings\Admin\Local Settings\Temp\rtf1.tmp

Creates: C:\Documents and Settings\Admin\dlst.dat

Opens: C:\WINDOWS\Prefetch\543BD82EC71AE746E83C14EBA2849-26981750.pf

Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\system32\imm32.dll

Opens: C:\WINDOWS\system32\urlmon.dll.123.Manifest
Opens: C:\WINDOWS\system32\urlmon.dll.123.Config
Opens: C:\WINDOWS\WinSxS\x86\_Microsoft.Windows.Common-

Controls\_6595b64144ccf1df\_6.0.2600.5512\_x-ww\_35d4ce83

Opens: 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:mylib\myfile

Opens: C:\WINDOWS\Temp\543bd82ec71ae746e83c14eba28494df.exe

Opens: C:\WINDOWS\system32\apphelp.dll
Opens: C:\WINDOWS\AppPatch\sysmain.sdb
Opens: C:\WINDOWS\AppPatch\systest.sdb

Opens: C:\WINDOWS\Temp

Opens: C:\

Opens: C:\WINDOWS

Opens: C:\windows\temp\543bd82ec71ae746e83c14eba28494df.exe.Manifest

 $\begin{array}{lll} \mbox{Opens:} & \mbox{C:\MINDOWS\system32\ws2\_32.dl1} \\ \mbox{Opens:} & \mbox{C:\MINDOWS\system32\ws2help.dl1} \\ \end{array}$ 

Opens: C:dlst.dat

Opens: C:\WINDOWS\Temp\58be9f66-5664-4dba-bd69-e7a34be8b0af
Opens: C:\Documents and Settings\Admin\Local Settings\Temp

Opens: C:\WINDOWS\regedit.exe

C:flh.dat Opens: Opens: C:pconfig C:dpconfig Opens:

Opens: C:\WINDOWS\system32\mswsock.dll Opens: C:\WINDOWS\system32\hnetcfg.dll Opens: C:\WINDOWS\system32\wshtcpip.dll C:\WINDOWS\regedit.exe.Manifest Opens: Opens: C:\WINDOWS\regedit.exe.Config

C:\WINDOWS\Prefetch\REGEDIT.EXE-1B606482.pf Opens:

Opens:

Opens: C:\WINDOWS\AppPatch C:\WINDOWS\Microsoft.NET Opens:

Opens: C:\WINDOWS\Microsoft.NET\Framework Opens: C:\WINDOWS\Microsoft.NET\Framework\v3.0

Opens: C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Workflow Foundation

Opens: C:\WINDOWS\system32 Opens: C:\WINDOWS\WinSxS

Opens: C:\WINDOWS\system32\ntdll.dll Opens: C:\WINDOWS\system32\kernel32.dll Opens: C:\WINDOWS\system32\unicode.nls Opens: C:\WINDOWS\system32\locale.nls Opens: C:\WINDOWS\system32\sorttbls.nls Opens: C:\WINDOWS\system32\msvcrt.dll Opens: C:\WINDOWS\system32\advapi32.dll Opens: C:\WINDOWS\system32\rpcrt4.dll Opens: C:\WINDOWS\system32\secur32.dll Opens: C:\WINDOWS\system32\gdi32.dll Opens: C:\WINDOWS\system32\user32.dll Opens: C:\WINDOWS\svstem32\shlwapi.dll Opens: C:\WINDOWS\system32\comdlg32.dll Opens: C:\WINDOWS\system32\shell32.dll Opens: C:\WINDOWS\system32\authz.dll Opens: C:\WINDOWS\system32\aclui.dll Opens: C:\WINDOWS\system32\ole32.dll Opens: C:\WINDOWS\system32\oleaut32.dll Opens: C:\WINDOWS\system32\ulib.dll Opens: C:\WINDOWS\system32\clb.dll Opens: C:\WINDOWS\system32\shimeng.dll C:\WINDOWS\AppPatch\AcGenral.dll

Opens: Opens: C:\WINDOWS\system32\winmm.dll C:\WINDOWS\system32\msacm32.dll Opens: Opens: C:\WINDOWS\system32\version.dll Opens: C:\WINDOWS\system32\userenv.dll  ${\tt C:\WINDOWS\system32\uxtheme.dll}$ Opens: Opens: C:\WINDOWS\system32\ctype.nls Opens: C:\WINDOWS\system32\sortkey.nls C:\WINDOWS\system32\MSCTF.dll Opens: Opens: C:\WINDOWS\system32\MSCTFIME.IME C:\WINDOWS\system32\MSIMTF.dll Opens: Opens: C:\WINDOWS\system32\narrhook.dll Opens: C:\WINDOWS\system32\oleacc.dll Opens: C:\WINDOWS\system32\msvcp60.dll Opens: C:\WINDOWS\system32\oleaccrc.dll

C:\WINDOWS\system32\win32k.sys Opens: C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Workflow

Foundation\PerfCounters.reg

Opens:

C:\WINDOWS\system32\SHELL32.dll.124.Manifest Opens: C:\WINDOWS\system32\SHELL32.dll.124.Config Opens: C:\WINDOWS\system32\ACLUI.dll.123.Manifest Opens: Opens: C:\WINDOWS\system32\ACLUI.dll.123.Config

Opens: C:\Documents and Settings\Admin\Local Settings\Temp\rtf1.tmp Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\rtf1.tmp

Writes to: C:\Documents and Settings\Admin\dlst.dat

Reads from: C:\WINDOWS\Temp\543bd82ec71ae746e83c14eba28494df.exe

Reads from: C:\WINDOWS\Prefetch\REGEDIT.EXE-1B606482.pf

Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\rtf1.tmp

#### Network Events

31.193.4.140:9091 Connects to: Connects to: 255.255.255.255:9091

## Windows Registry Events

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

Creates kev: HKLM\software\microsoft\microsoft windows nt 4.0

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 Creates key: HKCU\software\microsoft\multimedia\audio compression manager\priority v4.00

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

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

options\543bd82ec71ae746e83c14eba28494df.exe

```
Opens key:
                          HKLM\system\currentcontrolset\control\terminal server
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcrt.dll
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\secur32.dll
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\winlogon
 Opens key:
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\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\system\currentcontrolset\control\safeboot\option
 Opens key:
                          HKLM\software\policies\microsoft\windows\safer\codeidentifiers
 Opens key:
                          HKCU\software\policies\microsoft\windows\safer\codeidentifiers
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\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\shlwapi.dll
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens kev:
options\normaliz.dll
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\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\system\currentcontrolset\control\error message instrument\
 Opens key:
                          HKLM\system\currentcontrolset\control\error message instrument
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\gre_initialize
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\compatibility32
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\ime compatibility
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\windows
 Opens key:
                          \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ performance
 Opens key:
                          HKLM\software\microsoft\ole
 Opens kev:
                          HKCR\interface
                          HKCR\interface\{00020400-0000-0000-c000-00000000046}
 Opens key:
 Opens key:
                          HKLM\software\microsoft\oleaut
 Opens key:
                          HKLM\software\microsoft\oleaut\userera
 Opens key:
                          HKCU\
 Opens key:
                          HKCU\software\policies\microsoft\control panel\desktop
 Opens kev:
                          HKCU\control panel\desktop
 Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comctl32.dll
 Opens key:
                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ advanced
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\languagepack
 Opens key:
                          HKCU\software\classes\
 Opens key:
                          HKCU\software\classes\protocols\name-space handler\
 Opens key:
                          HKCR\protocols\name-space handler
 Opens key:
                          HKCU\software\classes\protocols\name-space handler
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings
                          HKLM\software\microsoft\windows\currentversion\internet settings
 Opens key:
 Opens key:
                          \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\
 Opens key:
                          HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
 Opens key:
                          HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
 Opens key:
                          HKLM\software\microsoft\internet explorer\main\featurecontrol
 Opens key:
                          HKCU\software\microsoft\internet explorer\main\featurecontrol
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
```

Opens key: HKLM\software\microsoft\internet

```
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
                                                   HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\zonemap\domains\
   Opens key:
                                                   HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
   Opens key:
                                                   \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\zonemap\ranges\
                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\zonemap\ranges\
   Opens key:
                                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
   Opens key:
                                                  HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
   Opens key:
                                                  HKLM\system\currentcontrolset\control\wmi\security
   Opens key:
                                                   HKLM\system\currentcontrolset\control\session manager\appcertdlls
   Opens key:
                                                   HKLM\system\currentcontrolset\control\session manager\appcompatibility
   Opens kev:
                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\apphelp.dll
   Opens key:
                                                   HKLM\system\wpa\tabletpc
                                                   HKLM\system\wpa\mediacenter
   Opens key:
   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\543bd82ec71ae746e83c14eba28494df.exe
                                                  HKLM\software\policies\microsoft\windows\safer\levelobjects
   Opens key:
   Opens key:
                                                  HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
   Opens key:
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ paths \ \{dda3f824-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-441b-834d-d8cb-440b-834d-d8cb-440b-834d-d8cb-440b-834d-d8cb-440b-834d-d8cb-440b
be2efd2c1a33}
                                                   HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
   Opens key:
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}
   Opens key:
b813f72dbb91}
   Opens kev:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes \setminus \{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-4760-566-4760-b16d-4760-5660-566-5660-
7c29ddecae3f}
   Opens key:
085bcc18a68d}
   Opens kev:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}
   Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus urlzones
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
   Opens kev:
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:
Opens key:
HKLM \ software \ \ microsoft \ \ windows \ \ safer \ \ code identifiers \ \ 131072 \ \ paths
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
   Opens kev:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
   Opens kev:
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ \ 262144 \ paths
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
   Opens kev:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
                                                   HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
   Opens kev:
                                                   HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
   Opens kev:
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
   Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
   Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
   Opens key:
HKCU\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 kev:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones

Opens kev:

 $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus paths$ 

Opens kev:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes

Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones

Opens kev:

 $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus paths$ 

Opens key:

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

Opens key:

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

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

options\ws2help.dll

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

options\ws2\_32.dll

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

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9

Opens key:

Opens key:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000001 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000000 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000003 Opens kev:

Opens kev: 

Opens key: 

Opens key: Opens kev:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000000 Opens key:

Opens kev:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\00000004

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001 Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000003

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

Opens key: HKLM\software\microsoft\rpc

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

options\543bd82ec71ae746e83c14eba28494df.exe\rpcthreadpoolthrottle

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

Opens key: HKLM\software\sophos Opens key: HKLM\software\g data Opens key: HKLM\software\doctor web Opens key: HKLM\software\kasperskylab Opens key: HKLM\software\eset

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

Opens key:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-

c7d49d7cecdc}

Opens key:

 $HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{4fe87b73-b12e-47d6-82c4-47d6-8$ 

fb0d4cf73262}

Opens key:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{cac79791-bd6d-4f3e-bcad-

e3686652faee}

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

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

options\hnetcfg.dll

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

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

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

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\wshtcpip.dll

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

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

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

options\regedit.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\shell32.dll

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

options\comdlg32.dll

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

options\authz.dll

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

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

options\ulib.dll

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

options\clb.dll

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

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

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

options\userenv.dll

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

options\uxtheme.dll

Opens kev: HKLM\svstem\setup

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

Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts Opens key: HKLM\system\currentcontrolset\control\nls\language groups Opens key:  $HKLM \backslash software \backslash microsoft \backslash windows \ nt \backslash current version \backslash drivers 32$ 

Opens key:

 $HKLM \verb| system| current control \verb| media properties| private properties| joystick| winmm | media properties| to the first properties | media properties| to the first properties | media properties| to the first propertie$ Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache

Opens kev:

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

Opens key:

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

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

Opens key:

 $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. \ msgsm610$ 

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

Opens key:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1

Opens key:

 $\label{lem:hklm} \verb+Kklm/software/microsoft/audiocompression manager/driver cache/msacm.sl\_anet$ 

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2 Opens kev: Opens key:  $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. 13 acm$ 

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

Opens key:  $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}$ 

folders

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

Opens key: HKCU\software\microsoft\windows\currentversion\thememanager HKCU\software\microsoft\windows\currentversion\policies\system Opens key: Oueries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat] Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack] Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]

Oueries value:

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

HKLM\software\microsoft\windows Oueries value:  $\verb|nt\currentversion\gre_initialize[disablemetafiles]|\\$ Queries value: HKLM\software\microsoft\windows

nt\currentversion\compatibility32[543bd82ec71ae746e83c14eba28494df]

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

compatibility[543bd82ec71ae746e83c14eba28494df]

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[interfacehelperdisableall]

Queries value: HKCR\interface[interfacehelperdisableallforole32]
Queries value: HKCR\interface[interfacehelperdisabletypelib]
Queries value: HKCR\interface[interfacehelperdisabletypelib]
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\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
Queries value: HKLM\software\microsoft\windows\currentversion\internet

Queries value: HKLM\software\micr settings[disableimprovedzonecheck]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature\_protocol\_lockdown[543bd82ec71ae746e83c14eba28494df.exe]

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

ab78-1084642581fb]

Queries value: HKLM\system\currentcontrolset\control\wmi\security[0000000-0000-0000-

0000-000000000000]

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

manager[safeprocesssearchmode]

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

manager\appcompatibility[disableappcompat]

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

Oueries value:

 $\label{thm:local_equation} HKLM \software \parbon is considered and the local constraints of t$ 

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

Queries value:

 $\label{lem:hamman} HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33\}[itemdata]}$ 

Queries value:

Queries value:

Queries value:

Queries value:

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

Queries value:

Queries value:

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

Queries value:

Queries value:

Queries value:

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

Oueries value:

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

Queries value:

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{94e3e076-8f53-42a5-8411-426-8411-4268-8411-4268-8411$ 

085bcc18a68d}[itemsize] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[saferflags] Oueries value: b91490411bfc}[itemdata] Oueries value:  $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe$ b91490411bfc}[hashalg] Oueries value: b91490411bfc}[itemsize] Oueries value:  $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe$ b91490411bfc}[saferflags] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope] HKCU\software\microsoft\windows\currentversion\explorer\shell Queries value: folders[cache] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename] Queries value: Queries value: 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]  $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ (000000000001[packed catalog item]) \ details \ de$ Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000002[packedcatalogitem] Oueries value: Queries value: Queries value:  $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries \ 000000000005 \ [packed catalog item]$ Oueries value: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000007[packedcatalogitem] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000008[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000009[packedcatalogitem] Oueries 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] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[serial\_access\_num] Oueries value:  $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 [num\_catalog\_entries]$ Queries value:  $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace \_catalog5 \ catalog\_entries \ 00000000001 [library path]$ Queries value: Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog S \setminus catalog\_entries \setminus 000000000001[providerid]$ Queries value:  $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ (catalog\_entries \ 00000000001 \ [address family]$ Queries value:  $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace \_ catalog 5 \ catalog\_entries \ 000000000001 [supported names pace]$ Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[enabled] Queries 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\000000000001[storesserviceclassinfo] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000002[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]

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus name space\_catalog 5 \setminus catalog\_entries \setminus 00000000000002 [address family]$ 

Queries value:

Queries value:

```
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ namespace\_catalog \ namespace\_
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
   Oueries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ catalog\_entries \ 000000000003 \ [displaystring]
   Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000003 \ [supported name space]
   Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
   Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog \ catalog\_entries \ 000000000003 \ [storesservice class in fo]
   Queries 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:
                                           HKLM\software\microsoft\microsoft windows nt 4.0[oid]
   Oueries value:
                                           HKLM\software\microsoft\microsoft windows nt 4.0[gid]
   Queries value:
   Oueries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-4404, and the services \ tcpip \ parameters \ terrange \ terr
c7d49d7cecdc}[nameserver]
   Queries value:
c7d49d7cecdc}[dhcpnameserver]
   Oueries value:
fb0d4cf73262}[nameserver]
   Queries value:
fb0d4cf73262}[dhcpnameserver]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{cac79791-bd6d-4f3e-bcad-
e3686652faee}[nameserver]
   Queries value:
e3686652faee}[dhcpnameserver]
                                           HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
   Oueries 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]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
   Oueries value:
                                           HKLM\software\microsoft\windows
nt\currentversion\compatibility32[regedit]
                                           HKLM\software\microsoft\windows nt\currentversion\ime
   Oueries value:
compatibility[regedit]
   Oueries value:
                                           HKLM\system\setup[systemsetupinprogress]
   Queries value:
                                           HKLM\system\currentcontrolset\control\nls\locale[00000409]
   Oueries value:
                                           Queries 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]
                                           HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
   Oueries value:
   Oueries value:
                                           HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
   Queries value:
                                           HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
   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]
```

HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]

HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]

HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]

HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]

HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]

Oueries value:

Oueries value:

Queries value:

Oueries value:

Queries value:

```
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]
  Queries value:
                                    HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
  Oueries value:
                                    HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
  Queries value:
                                    HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
  Oueries value:
                                    HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
  Oueries value:
                                    HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
  Oueries value:
                                    HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
  Oueries value:
                                    HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
                                    HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
  Oueries value:
  Queries value:
                                    HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
  Oueries 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]
  Queries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
                                    HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
  Queries value:
  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[mixer4]
  Oueries value:
                                    HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
                                    HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
  Queries value:
                                    HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
  Queries value:
  Queries value:
                                    HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
                                    HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
  Queries value:
                                    HKCU\software\microsoft\multimedia\audio[systemformats]
  Queries value:
  Oueries 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\audiocompressionmanager\drivercache\msacm.imaadpcm[cfiltertags]
                                    HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msadpcm]
  Oueries 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[aformattagcache]
  Queries value:
Oueries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msg711]
  Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[fdwsupport]
  Queries value:
Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[aformattagcache]
  Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cfiltertags]
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msgsm610]
  Queries value:
HKLM \verb|\software\m| icrosoft\audiocompression manager\driver cache \verb|\m| sacm. msgsm610[fdwsupport]|
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cformattags]
  Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[aformattagcache]
  Queries value:
HKLM \verb|\software\microsoft\audiocompression manager\driver cache \verb|\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:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cformattags]
  Queries value:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.trspch[aformattagcache]
  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]
```

Queries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cformattags] Oueries value:  $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msg723[a formattag cache]$ Queries value:  $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. msg723[cfilter tags]$ Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msaudio1] Oueries value:  $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msaudio1[fdwsupport]$ Oueries value:  $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msaudio1[cformattags]$ Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[aformattagcache] Oueries value:  $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msaudio1[cfilter tags]$ HKLM\software\microsoft\windows Queries value: nt\currentversion\drivers32[msacm.sl anet] Queries value:  $HKLM \label{lem:hklm} Which is a constant, which is a constant, and it is a constant,$ Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl\_anet[cformattags] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl\_anet[aformattagcache] HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2] Oueries value: Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport] Oueries 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: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.13acm] HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.13acm[fdwsupport] Oueries value:  $HKLM \verb|\software\microsoft\audiocompressionmanager\drivercache\mbox| 13acm[cformattags]$ Queries value:  $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. 13 acm [a formattag cache]$ 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 Queries value: v4.00[priority1] Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[userenvdebuglevel] Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[chkaccdebuglevel] HKLM\system\currentcontrolset\control\productoptions[producttype] Oueries value: Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[personal] HKCU\software\microsoft\windows\currentversion\explorer\user shell Oueries value: folders[local settings] Oueries value: HKLM\software\microsoft\windows 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] Sets/Creates value: HKLM\software\microsoft\microsoft windows nt 4.0[guid] HKCU\software\microsoft\windows\currentversion\run[dskchk] Sets/Creates value: Value changes: HKLM\software\microsoft\cryptography\rng[seed] Value changes: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[dhcpnameserver] Value changes: -HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3

c7d49d7cecdc}[nameserver]