Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 56, Task ID: 223

Task ID:	223
Risk Level:	5
Date Processed:	2016-04-28 12:53:28 (UTC)
Processing Time:	61.39 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\600ecbc03600897002c1a0aba17ea3bd.exe"
Sample ID:	56
Type:	basic
Owner:	admin
Label:	600ecbc03600897002c1a0aba17ea3bd
Date Added:	2016-04-28 12:44:55 (UTC)
File Type:	PE32:win32:gui
File Size:	393216 bytes
MD5:	600ecbc03600897002c1a0aba17ea3bd
SHA256:	ca2c2aa89e584bfd63d133f071cf4d1a4789c161179f5beb8b9926f674fe3760
Description:	None

Pattern Matching Results

5 Packer: UPX
2 PE: Nonstandard section
5 Creates process in suspicious location
5 PE: Contains compressed section
5 Resource section contains an executable

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Resource section contains an executable
Anomaly:	PE: Contains one or more non-standard sections
Packer:	UPX

Process/Thread Events

Creates process: C:\WINDOWS\Temp\600ecbc03600897002c1a0aba17ea3bd.exe ["c:\windows\temp\600ecbc03600897002c1a0aba17ea3bd.exe"]

Creates process: C:\DOCUME~1\Admin\LOCALS~1\Temp\SSESTART\Setup.exe [C:\DOCUME~1\Admin\LOCALS~1\Temp\SSESTART\Setup.exe c:\windows\temp\SSEset.dat /BS]

Named Object Events

Creates mutex: \BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003

Creates mutex: \BaseNamedObjects_MSIExecute

Creates mutex: \BaseNamedObjects\SHIMLIB_LOG_MUTEX

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

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

Creates semaphore: \BaseNamedObjects\C:?WINDOWS?TEMP?600ECBC03600897002C1A0ABA17EA3BD.EXE

Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore: \BaseNamedObjects\C:?DOCUME~1?ADMIN?LOCALS~1?TEMP?SSESTART?SETUP.EXE

File System Events

Creates: C:\Documents and Settings\Admin\Local Settings\Temp\SSESTART
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\SSESTART\Setup.exe
Opens: C:\WINDOWS\Prefetch\600ECBC03600897002C1A0ABA17EA-21FE3426.pf
Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\system32\msvbvm60.dll
Opens: C:\WINDOWS\system32\imm32.dll
Opens: C:\WINDOWS\system32\rpcss.dll
Opens: C:\WINDOWS\system32\MSCTF.dll
Opens: C:\WINDOWS\system32\sxs.dll
Opens: C:\WINDOWS\system32\MSCTFIME.IME
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\SSESTART\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\SSESTART
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\SSESTART\Setup.exe
Opens: C:\WINDOWS\system32\apphelp.dll
Opens: C:\WINDOWS\AppPatch\sysmain.sdb
Opens: C:\WINDOWS\AppPatch\systest.sdb
Opens: C:\
Opens: C:\Documents and Settings
Opens: C:\Documents and Settings\Admin\Local Settings
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\SSESTART\Setup.exe.Manifest
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\SSESTART\Setup.exe.Config
Opens: C:\WINDOWS\Prefetch\SETUP.EXE-22C4D4E4.pf
Opens: C:\WINDOWS\system32\shimeng.dll
Opens: C:\WINDOWS\AppPatch\AcGenral.dll
Opens: C:\WINDOWS\system32\winmm.dll
Opens: C:\WINDOWS\system32\msacm32.dll
Opens: C:\WINDOWS\system32\uxtheme.dll
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\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\Fonts\sserife.fon
Opens: C:\WINDOWS\Fonts\arialbd.ttf
Opens: C:\WINDOWS\Temp
Opens: C:\windows\temp\SSEset.dat
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\SSESTART\Setup.exe

Windows Registry Events

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
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\600ecbc03600897002c1a0aba17ea3bd.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\gdi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\user32.dll
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\imm32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntdll.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\secur32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rpcrt4.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\advapi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ole32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\oleaut32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvbvm60.dll
Opens key: HKLM\system\currentcontrolset\control\error message instrument\
Opens key: HKLM\system\currentcontrolset\control\error message instrument
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility
Opens key: HKLM\software\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\microsoft\windows nt\currentversion\winlogon
Opens key: HKLM\
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\software\microsoft\ole
Opens key: HKCR\interface
Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}
Opens key: HKLM\software\microsoft\oleaut
Opens key: HKLM\software\microsoft\oleaut\userera
Opens key: HKCU\
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msctf.dll
Opens key: HKLM\software\microsoft\ctf\compatibility\600ecbc03600897002c1a0aba17ea3bd.exe
Opens key: HKLM\software\microsoft\ctf\systemshared\
Opens key: HKCU\keyboard layout\toggle
Opens key: HKLM\software\microsoft\ctf\
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\sxs.dll
Opens key: HKLM\system\setup
Opens key: HKLM\software\microsoft\windows nt\currentversion\imm
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\version.dll
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msctfime.ime
Opens key: HKCU\software\microsoft\ctf
Opens key: HKLM\software\microsoft\ctf\systemshared
Opens key: HKLM\system\currentcontrolset\control\nls\codepage
Opens key: HKLM\software\microsoft\vba\monitors
Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\apphelp.dll

Opens key: HKLM\system\wpa\tabletpc
Opens key: HKLM\system\wpa\mediacenter
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\setup.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\software\policies\microsoft\windows\safer\levelobjects
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\setup.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\shlwapi.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shell32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\userenv.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\drivers32
Opens key:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache
Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm
Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711
Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723
Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1
Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm
Opens key: HKLM\system\currentcontrolset\control\mediaresources\acm
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance
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: HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack
Opens key: HKLM\system\currentcontrolset\control\productoptions
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders
Opens key: HKLM\software\policies\microsoft\windows\system
Opens key: HKCU\software\microsoft\windows\currentversion\thememanager
Opens key: HKLM\software\microsoft\ctf\compatibility\setup.exe
Opens key: HKCU\software\microsoft\ctf\langbaraddin\
Opens key: HKLM\software\microsoft\ctf\langbaraddin\
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[600ecbc03600897002c1a0aba17ea3bd]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[600ecbc03600897002c1a0aba17ea3bd]
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
Queries value: HKLM\system\currentcontrolset\control\session manager[criticalsectiontimeout]
Queries value: HKLM\software\microsoft\ole[rwlockresourcetimeout]
Queries value: HKCR\interface[interfacehelperdisableall]
Queries value: HKCR\interface[interfacehelperdisableallforole32]
Queries value: HKCR\interface[interfacehelperdisabletypelib]
Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperdisableall]
Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperdisableallforole32]
Queries value: HKCU\control panel\desktop[multiuilanguageid]
Queries value: HKLM\software\microsoft\ctf\systemshared[cuas]
Queries value: HKCU\keyboard layout\toggle[language hotkey]
Queries value: HKCU\keyboard layout\toggle[hotkey]
Queries value: HKCU\keyboard layout\toggle[layout hotkey]
Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]
Queries value: HKLM\system\currentcontrolset\control\session manager[safeprocesssearchmode]
Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
Queries value: HKCU\software\microsoft\ctf[disable thread input manager]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[932]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[949]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[950]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[936]
Queries value: HKLM\system\currentcontrolset\control\session manager\appcompatibility[disableappcompat]
Queries value: HKLM\system\wpa\mediacenter[installed]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}[itemdata]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}[saferflags]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[itemdata]
Queries 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]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[itemsize]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[itemsize]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[itemsize]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[itemsize]
Queries value:
HKLM\software\policies\microsoft\windows\safer\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]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cache]
Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\setup.exe[debugger]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\setup.exe[executeoptions]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\setup.exe[disableheaplookaside]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\setup.exe[shutdownflags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\setup.exe[minimumstackcommitinbytes]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\setup.exe[globalflag]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\setup.exe[debugprocessheaponly]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[setup]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[setup]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
Queries 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]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
Queries 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]
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[mixer5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
Queries value: 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]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[aformattagcache]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cfiltertags]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msadpcm]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[fdwsupport]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cformattags]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[aformattagcache]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cfiltertags]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msg711]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[fdwsupport]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cformattags]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[aformattagcache]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cfiltertags]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msgsm610]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[fdwsupport]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cformattags]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[aformattagcache]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cfiltertags]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.trspch]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cformattags]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[aformattagcache]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cfiltertags]
Queries value: HKLM\software\microsoft\windows
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]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[aformattagcache]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cfiltertags]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msaudio1]
Queries 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]
Queries 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]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cformattags]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[aformattagcache]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cformattags]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[aformattagcache]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.l3acm]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[fdwsupport]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cformattags]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[aformattagcache]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags]
Queries value: HKCU\software\microsoft\multimedia\audio compression
manager\msacm[nopcmconverter]
Queries value: HKCU\software\microsoft\multimedia\audio compression manager\priority
v4.00[priority1]
Queries value: HKLM\system\setup[systemsetupinprogress]
Queries value: HKCU\control panel\desktop[smoothscroll]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\winlogon[chkaccdebuglevel]
Queries value: HKLM\system\currentcontrolset\control\productoptions[producttype]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[personal]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local settings]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\winlogon[rsopdebuglevel]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
Queries value: HKCU\control panel\desktop[lamebuttontext]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]