Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 84, Task ID: 335

Task ID:	335
Risk Level:	5
Date Processed:	2016-04-28 12:56:13 (UTC)
Processing Time:	61.09 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\90d0d029326bfb8fd9a1a94749386ca7.exe"

Sample ID:	84
Type:	basic
Owner:	admin
Label:	90d0d029326bfb8fd9a1a94749386ca7
Date Added:	2016-04-28 12:44:58 (UTC)
File Type:	PE32:win32:gui
File Size:	601784 bytes
MD5:	90d0d029326bfb8fd9a1a94749386ca7
SHA256:	fb49f75f321fda6837a8e43228e50ecb68c9fdf7824d1425ac5a1a5b8c80ee00
Description:	None

Pattern Matching Results

5	Possible injector
2	PE: Nonstandard section
5	Packer: UPX
5	PE: Contains compressed section

Static Events

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

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\90d0d029326bfb8fd9a1a94749386ca7.exe ["c:\windows\temp\90d0d029326bfb8fd9a1a94749386ca7.exe"]

Named Object Events

Creates mutex:	\BaseNamedObjects\DDrawWindowListMutex
Creates mutex:	\BaseNamedObjects\DDrawDriverObjectListMutex
Creates mutex:	\BaseNamedObjects__DDrawExclMode__
Creates mutex:	\BaseNamedObjects__DDrawCheckExclMode__
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\DirectSound DllMain mutex (0x0000051C)
Creates mutex:	\BaseNamedObjects\DirectMusicMasterClockMutex
Creates mutex:	\BaseNamedObjects\DirectSound Administrator shared thread array (lock)
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.IGH
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

```
  Creates:              C:\Documents and Settings\Admin\Local Settings\Temp\MMBPlayer
  Opens:                C:\WINDOWS\Prefetch\90D0D029326BFB8FD9A1A94749386-248514FC.pf
  Opens:                C:\Documents and Settings\Admin
  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\system32\msacm32.dll
  Opens:                C:\WINDOWS\system32\winmm.dll
  Opens:                C:\WINDOWS\system32\oledlg.dll
  Opens:                C:\WINDOWS\system32\olepro32.dll
  Opens:                C:\WINDOWS\system32\winspool.drv
  Opens:                C:\WINDOWS\Temp\90d0d029326bfb8fd9a1a94749386ca7.exe
  Opens:                C:\WINDOWS\system32\imm32.dll
  Opens:                C:\WINDOWS\WindowsShell.Manifest
  Opens:                C:\WINDOWS\WindowsShell.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\ddraw.dll
  Opens:                C:\WINDOWS\system32\dciman32.dll
  Opens:                C:\WINDOWS\win.ini
  Opens:                C:\WINDOWS\system32\rpcss.dll
  Opens:                C:\WINDOWS\system32\MSCTF.dll
  Opens:                C:\WINDOWS\system32\clbcatq.dll
  Opens:                C:\WINDOWS\system32\comres.dll
  Opens:                C:\WINDOWS\Registration\R000000000007.clb
  Opens:                C:\WINDOWS\system32\dmusic.dll
  Opens:                C:\WINDOWS\system32\dsound.dll
  Opens:                C:\WINDOWS\system32\setupapi.dll
  Opens:                C:\WINDOWS\system32\wintrust.dll
  Opens:                C:\WINDOWS\system32\crypt32.dll
  Opens:                C:\WINDOWS\system32\msasn1.dll
  Opens:                C:\WINDOWS\system32\d3d8.dll
  Opens:                C:\WINDOWS\system32\d3d8thk.dll
  Opens:                C:\WINDOWS\system32\dpnhpast.dll
  Opens:                C:\WINDOWS\system32\rsaenh.dll
  Opens:                C:\
  Opens:                C:\WINDOWS\Fonts\sserife.fon
  Opens:                C:\WINDOWS\system32\MSCTFIME.IME
  Opens:                C:\WINDOWS\system32\MSIMTF.dll
  Opens:                C:\WINDOWS\system32\d3d9.dll
  Opens:                C:\WINDOWS\system32\uxtheme.dll
  Reads from:           C:\WINDOWS\Temp\90d0d029326bfb8fd9a1a94749386ca7.exe
  Reads from:           C:\WINDOWS\win.ini
  Reads from:           C:\WINDOWS\Registration\R000000000007.clb
  Reads from:           C:\WINDOWS\system32\rsaenh.dll
```

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
  Creates key:          HKLM\software\microsoft\directdraw\mostrecentapplication
  Creates key:          HKLM\system\currentcontrolset\control\deviceclasses
  Creates key:          HKLM\software\microsoft\direct3d\mostrecentapplication
  Creates key:          HKCU\software\mediachance
  Creates key:          HKCU\software\mediachance\multimedia player
  Creates key:          HKCU\software\mediachance\multimedia player\font
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\90d0d029326bfb8fd9a1a94749386ca7.exe
  Opens key:                HKLM\system\currentcontrolset\control\terminal server
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  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\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:                HKLM\
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\diagnostics
  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\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\gdi32.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\comctl32.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\comdlg32.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\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\oledlg.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\olepro32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winspool.drv
  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\currentversion\explorer\performance
  Opens key:                HKCU\
  Opens key:                HKCU\software\policies\microsoft\control panel\desktop
  Opens key:                 HKCU\control panel\desktop
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\languagepack
  Opens key:                 HKLM\system\setup
  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\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\software\classes\
  Opens key:                 HKCU\software\classes\clsid
  Opens key:                 HKCR\clsid
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dciman32.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ddraw.dll
  Opens key:                 HKLM\hardware\devicemap\video
  Opens key:                 HKLM\software\microsoft\directdraw\compatibility
  Opens key:                 HKLM\software\microsoft\directdraw\compatibility\bug!
  Opens key:                 HKLM\software\microsoft\directdraw\compatibility\demolitionderby2
  Opens key:                 HKLM\software\microsoft\directdraw\compatibility\mortalkombat3
  Opens key:                 HKLM\software\microsoft\directdraw\compatibility\msgolf98
  Opens key:                 HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay
  Opens key:                 HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo
  Opens key:                 HKLM\software\microsoft\directdraw\compatibility\rogue squadron
  Opens key:                 HKLM\software\microsoft\directdraw\compatibility\savage
  Opens key:                 HKLM\software\microsoft\directdraw\compatibility\scorchedplanet
  Opens key:                 HKLM\software\microsoft\directdraw\compatibility\silentthunder
  Opens key:                 HKLM\software\microsoft\directdraw\compatibility\terracide
  Opens key:                 HKLM\software\microsoft\directdraw\compatibility\thirddimension
  Opens key:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark
  Opens key:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark
  Opens key:                 HKLM\software\microsoft\directdraw\gammacalibrator
  Opens key:                 HKLM\software\microsoft\directdraw
  Opens key:                 HKLM\software\microsoft\direct3d
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
  Opens key:
HKLM\software\microsoft\ctf\compatibility\90d0d029326bfb8fd9a1a94749386ca7.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\com3
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comres.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\clbcatq.dll
  Opens key:                HKLM\software\microsoft\com3\debug
  Opens key:                HKLM\software\classes
  Opens key:                HKU\
  Opens key:                HKCU\software\classes\clsid\{636b9f10-0c7d-11d1-95b2-0020afdc7421}
  Opens key:                HKCR\clsid\{636b9f10-0c7d-11d1-95b2-0020afdc7421}
  Opens key:                HKCU\software\classes\clsid\{636b9f10-0c7d-11d1-95b2-
0020afdc7421}\treatas
  Opens key:                HKCR\clsid\{636b9f10-0c7d-11d1-95b2-0020afdc7421}\treatas
  Opens key:                HKCU\software\classes\clsid\{636b9f10-0c7d-11d1-95b2-
0020afdc7421}\inprocserver32
  Opens key:                HKCR\clsid\{636b9f10-0c7d-11d1-95b2-0020afdc7421}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{636b9f10-0c7d-11d1-95b2-
0020afdc7421}\inprocserverx86
  Opens key:                HKCR\clsid\{636b9f10-0c7d-11d1-95b2-0020afdc7421}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{636b9f10-0c7d-11d1-95b2-
0020afdc7421}\localserver32
  Opens key:                HKCR\clsid\{636b9f10-0c7d-11d1-95b2-0020afdc7421}\localserver32
  Opens key:                HKCU\software\classes\clsid\{636b9f10-0c7d-11d1-95b2-
0020afdc7421}\inprochandler32
  Opens key:                HKCR\clsid\{636b9f10-0c7d-11d1-95b2-0020afdc7421}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{636b9f10-0c7d-11d1-95b2-
0020afdc7421}\inprochandlerx86
  Opens key:                HKCR\clsid\{636b9f10-0c7d-11d1-95b2-0020afdc7421}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{636b9f10-0c7d-11d1-95b2-
0020afdc7421}\localserver
  Opens key:                HKCR\clsid\{636b9f10-0c7d-11d1-95b2-0020afdc7421}\localserver
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dsound.dll
  Opens key:                HKLM\software\microsoft\directx
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dmusic.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\setupapi.dll
  Opens key:                HKLM\system\currentcontrolset\control\minint
  Opens key:                HKLM\system\wpa\pnp
  Opens key:                HKLM\software\microsoft\windows\currentversion\setup
  Opens key:                HKLM\software\microsoft\windows\currentversion
  Opens key:                HKLM\software\microsoft\windows\currentversion\setup\apploglevels
  Opens key:                HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters
  Opens key:                HKLM\software\policies\microsoft\system\dnsclient
  Opens key:                HKLM\software\microsoft\rpc\pagedbuffers
  Opens key:                HKLM\software\microsoft\rpc
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\90d0d029326bfb8fd9a1a94749386ca7.exe\rpcthreadpoolthrottle
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                HKLM\system\currentcontrolset\control\computername
  Opens key:                HKLM\system\currentcontrolset\control\deviceclasses\{6994ad04-93ef-11d0-
a3cc-00a0c9223196}
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msasn1.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\crypt32.dll
  Opens key:                HKLM\system\currentcontrolset\services\crypt32\performance
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\msasn1
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imagehlp.dll
```

```
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wintrust.dll
  Opens key:                HKLM\software\microsoft\directmusic\defaults
  Opens key:                HKLM\software\microsoft\directmusic
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\d3d8thk.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\d3d8.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dpnhpast.dll
  Opens key:                HKCU\software\microsoft\cryptography\providers\type 001
  Opens key:                HKLM\software\microsoft\cryptography\defaults\provider types\type 001
  Opens key:                HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rsaenh.dll
  Opens key:                HKLM\software\policies\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography\offload
  Opens key:                HKCU\software
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\imm
  Opens key:                HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctfime.ime
  Opens key:                HKCU\software\microsoft\ctf
  Opens key:                HKLM\software\microsoft\ctf\systemshared
  Opens key:                HKCU\software\microsoft\multimedia\sound mapper
  Opens key:                HKCU\software\microsoft\windows\currentversion\multimedia\midimap
  Opens key:
HKLM\system\currentcontrolset\control\mediaresources\directsound\application
compatibility\90d0d029326bfb8fd9a1a94749386ca7.exe436f524400092eb8
  Opens key:                HKLM\system\currentcontrolset\control\deviceclasses\{a7c7a5b1-5af3-11d1-
9ced-00a024bf0407}
  Opens key:                HKLM\system\currentcontrolset\control\mediaresources
  Opens key:                HKLM\system\currentcontrolset\control\mediaresources\directsound
  Opens key:                HKLM\system\currentcontrolset\control\mediaresources\directsound\device
presence
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
  Opens key:                HKCU\software\microsoft\windows\currentversion\thememanager
  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\terminal server[tsuserenabled]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
  Queries value:            HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\compatibility32[90d0d029326bfb8fd9a1a94749386ca7]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[90d0d029326bfb8fd9a1a94749386ca7]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
  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\system\setup[systemsetupinprogress]
  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\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:            HKLM\hardware\devicemap\video[maxobjectnumber]
  Queries value:            HKLM\hardware\devicemap\video[\device\video0]
  Queries value:            HKLM\hardware\devicemap\video[\device\video1]
  Queries value:            HKLM\hardware\devicemap\video[\device\video2]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\bug![name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\bug![flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\bug![id]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[id]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[id]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\msgolf98[name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\msgolf98[flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\msgolf98[id]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[id]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[id]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\rogue squadron[name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\rogue squadron[flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\rogue squadron[id]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\savage[name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\savage[flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\savage[id]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[id]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\silentthunder[name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\silentthunder[flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\silentthunder[id]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\terracide[name]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\terracide[flags]
  Queries value:            HKLM\software\microsoft\directdraw\compatibility\terracide[id]
```

```
 Queries value:            HKLM\software\microsoft\directdraw\compatibility\thirddimension[name]
 Queries value:            HKLM\software\microsoft\directdraw\compatibility\thirddimension[flags]
 Queries value:            HKLM\software\microsoft\directdraw\compatibility\thirddimension[id]
 Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[name]
 Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[flags]
 Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[id]
 Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[name]
 Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[flags]
 Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[id]
 Queries value:            HKLM\software\microsoft\directdraw[modexonly]
 Queries value:            HKLM\software\microsoft\directdraw[emulationonly]
 Queries value:            HKLM\software\microsoft\directdraw[showframerate]
 Queries value:            HKLM\software\microsoft\directdraw[enableprintscreen]
 Queries value:            HKLM\software\microsoft\directdraw[forceagpsupport]
 Queries value:            HKLM\software\microsoft\directdraw[disableagpsupport]
 Queries value:            HKLM\software\microsoft\directdraw[disablemmx]
 Queries value:            HKLM\software\microsoft\directdraw[disableddscapsinddsd]
 Queries value:            HKLM\software\microsoft\directdraw[disablewidersurfaces]
 Queries value:            HKLM\software\microsoft\directdraw[usenonlocalvidmem]
 Queries value:            HKLM\software\microsoft\directdraw[forcerefreshrate]
 Queries value:            HKLM\software\microsoft\direct3d[flipnovsync]
 Queries value:            HKLM\software\microsoft\ctf\systemshared[cuas]
 Queries value:            HKCU\keyboard layout\toggle[language hotkey]
 Queries value:            HKCU\keyboard layout\toggle[hotkey]
 Queries value:            HKCU\keyboard layout\toggle[layout hotkey]
 Queries value:            HKLM\software\microsoft\ctf[enableanchorcontext]
 Queries value:            HKLM\software\microsoft\com3[com+enabled]
 Queries value:            HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
 Queries value:            HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]
 Queries value:            HKLM\software\microsoft\com3[regdbversion]
 Queries value:            HKCR\clsid\{636b9f10-0c7d-11d1-95b2-
0020afdc7421}\inprocserver32[inprocserver32]
 Queries value:            HKCR\clsid\{636b9f10-0c7d-11d1-95b2-0020afdc7421}\inprocserver32[]
 Queries value:            HKCR\clsid\{636b9f10-0c7d-11d1-95b2-0020afdc7421}[appid]
 Queries value:            HKCR\clsid\{636b9f10-0c7d-11d1-95b2-
0020afdc7421}\inprocserver32[threadingmodel]
 Queries value:            HKLM\software\microsoft\directx[glitchinstrumentation]
 Queries value:            HKLM\system\wpa\pnp[seed]
 Queries value:            HKLM\system\setup[osloaderpath]
 Queries value:            HKLM\system\setup[systempartition]
 Queries value:            HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
 Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
 Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]
 Queries value:            HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
 Queries value:            HKLM\software\microsoft\windows\currentversion[devicepath]
 Queries value:            HKLM\software\microsoft\windows\currentversion\setup[loglevel]
 Queries value:            HKLM\software\microsoft\windows\currentversion\setup[logpath]
 Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
 Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
 Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
 Queries value:            HKLM\software\microsoft\rpc[maxrpcsize]
 Queries value:            HKLM\software\microsoft\directmusic\defaults[usepentiumclock]
 Queries value:            HKLM\software\microsoft\directmusic[defaulttomskernelsynth]
 Queries value:            HKLM\software\microsoft\directmusic[disablehwacceleration]
```

```
  Queries value:            HKLM\software\microsoft\direct3d[disablemmx]
  Queries value:            HKLM\software\microsoft\cryptography\defaults\provider types\type
001[name]
  Queries value:            HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
  Queries value:            HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  Queries value:            HKLM\software\microsoft\cryptography[machineguid]
  Queries value:            HKCU\software\mediachance\multimedia player\font[height]
  Queries value:            HKCU\software\mediachance\multimedia player\font[width]
  Queries value:            HKCU\software\mediachance\multimedia player\font[escape]
  Queries value:            HKCU\software\mediachance\multimedia player\font[orient]
  Queries value:            HKCU\software\mediachance\multimedia player\font[weight]
  Queries value:            HKCU\software\mediachance\multimedia player\font[italic]
  Queries value:            HKCU\software\mediachance\multimedia player\font[name]
  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\mediaresources\directsound\device
presence[wdm]
  Queries value:            HKLM\system\currentcontrolset\control\mediaresources\directsound\device
presence[vxd]
  Queries value:            HKLM\system\currentcontrolset\control\mediaresources\directsound\device
presence[emulated]
  Queries value:            HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
  Queries value:            HKCU\control panel\desktop[lamebuttontext]
  Value changes:            HKLM\software\microsoft\cryptography\rng[seed]
  Value changes:            HKLM\software\microsoft\directdraw\mostrecentapplication[name]
  Value changes:            HKLM\software\microsoft\directdraw\mostrecentapplication[id]
  Value changes:            HKLM\software\microsoft\direct3d\mostrecentapplication[name]
```