Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	334
Risk Level:	5
Date Processed:	2016-04-28 12:56:09 (UTC)
Processing Time:	61.55 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:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\__DDrawExclMode__
Creates mutex:	\Sessions\1\BaseNamedObjects\__DDrawCheckExclMode__
Creates mutex:	\Sessions\1\BaseNamedObjects\DDrawWindowListMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\DDrawDriverObjectListMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\DirectSound DllMain mutex (0x00000B1C)
Creates mutex:	\Sessions\1\BaseNamedObjects\DirectMusicMasterClockMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\DirectSound Administrator shared thread array (lock)
Creates event:	\Sessions\1\BaseNamedObjects\DINPUTWINMM

File System Events

Creates:	C:\Users\Admin\AppData\Local\Temp\MMBPlayer
Opens:	C:\Windows\Prefetch\90D0D029326BFB8FD9A1A94749386-2250CC38.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\90d0d029326bfb8fd9a1a94749386ca7.exe
Opens:	C:\Windows\SysWOW64\ntdll.dll

```
  Opens:                 C:\Windows\SysWOW64\kernel32.dll
  Opens:                 C:\Windows\SysWOW64\KernelBase.dll
  Opens:                 C:\Windows\apppatch\sysmain.sdb
  Opens:                 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985
  Opens:                 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll
  Opens:                 C:\Windows\SysWOW64\msacm32.dll
  Opens:                 C:\Windows\SysWOW64\oledlg.dll
  Opens:                 C:\Windows\SysWOW64\olepro32.dll
  Opens:                 C:\Windows\SysWOW64\version.dll
  Opens:                 C:\Windows\SysWOW64\winmm.dll
  Opens:                 C:\Windows\SysWOW64\winspool.drv
  Opens:                 C:\Windows\SysWOW64\sechost.dll
  Opens:                 C:\Windows\SysWOW64\combase.dll
  Opens:                 C:\Windows\SysWOW64\winmmbase.dll
  Opens:                 C:\Windows\SysWOW64\SHCore.dll
  Opens:                 C:\Windows\SysWOW64\msvcrt.dll
  Opens:                 C:\Windows\SysWOW64\bcryptprimitives.dll
  Opens:                 C:\Windows\SysWOW64\cryptbase.dll
  Opens:                 C:\Windows\SysWOW64\sspicli.dll
  Opens:                 C:\Windows\SysWOW64\rpcrt4.dll
  Opens:                 C:\Windows\SysWOW64\advapi32.dll
  Opens:                 C:\Windows\SysWOW64\user32.dll
  Opens:                 C:\Windows\SysWOW64\gdi32.dll
  Opens:                 C:\Windows\SysWOW64\shlwapi.dll
  Opens:                 C:\Windows\SysWOW64\shell32.dll
  Opens:                 C:\Windows\SysWOW64\comdlg32.dll
  Opens:                 C:\Windows\SysWOW64\ole32.dll
  Opens:                 C:\Windows\SysWOW64\oleaut32.dll
  Opens:                 C:\Windows\SysWOW64\imm32.dll
  Opens:                 C:\Windows\SysWOW64\msctf.dll
  Opens:                 C:\Windows\WindowsShell.Manifest
  Opens:                 C:\Windows\SysWOW64\ddraw.dll
  Opens:                 C:\Windows\SysWOW64\dciman32.dll
  Opens:                 C:\Windows\win.ini
  Opens:                 C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                 C:\Windows\SysWOW64\uxtheme.dll
  Opens:                 C:\Windows\SysWOW64\d3d10warp.dll
  Opens:                 C:\Windows\SysWOW64\clbcatq.dll
  Opens:                 C:\Windows\SysWOW64\dmusic.dll
  Opens:                 C:\Windows\SysWOW64\ksuser.dll
  Opens:                 C:\Windows\SysWOW64\dsound.dll
  Opens:                 C:\Windows\SysWOW64\powrprof.dll
  Opens:                 C:\Windows\SysWOW64\cfgmgr32.dll
  Opens:                 C:\Windows\SysWOW64\devobj.dll
  Opens:                 C:\Windows\SysWOW64\setupapi.dll
  Opens:                 C:\Windows\SysWOW64\msasn1.dll
  Opens:                 C:\Windows\SysWOW64\crypt32.dll
  Opens:                 C:\Windows\SysWOW64\wintrust.dll
  Opens:                 C:\Windows\SysWOW64\en-US\dmusic.dll.mui
  Opens:                 C:\Windows\SysWOW64\d3d8.dll
  Opens:                 C:\Windows\SysWOW64\d3d8thk.dll
  Opens:                 C:\Windows\SysWOW64\dwmapi.dll
  Opens:                 C:\Windows\SysWOW64\dpnhpast.dll
  Opens:                 C:\Windows\SysWOW64\tzres.dll
  Opens:                 C:\Windows\SysWOW64\en-US\tzres.dll.mui
  Opens:                 C:\
  Opens:                 C:\Windows\Fonts\sserife.fon
  Opens:                 C:\Windows\SysWOW64\MMDevAPI.dll
  Opens:                 C:\Windows\SysWOW64\d3d9.dll
  Opens:                 C:\Windows\SysWOW64\en-US\dsound.dll.mui
  Opens:                 C:\Windows\Fonts\StaticCache.dat
  Opens:                  C:\Windows\SysWOW64\imageres.dll
  Reads from:             C:\Windows\win.ini
  Reads from:             C:\Windows\Temp\90d0d029326bfb8fd9a1a94749386ca7.exe
  Reads from:             C:\Windows\Fonts\StaticCache.dat
```

Windows Registry Events

```
  Creates key:            HKLM\software\wow6432node\microsoft\directdraw\mostrecentapplication
  Creates key:            HKLM\software\wow6432node\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\wow64
  Opens key:              HKLM\system\currentcontrolset\control\terminal server
  Opens key:              HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:              HKLM\system\currentcontrolset\control\srp\gp\dll
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
  Opens key:              HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:              HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:              HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:              HKLM\system\currentcontrolset\control\nls\language
  Opens key:              HKLM\system\currentcontrolset\control\mui\uilanguages
  Opens key:              HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
  Opens key:              HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
  Opens key:              HKLM\software\wow6432node\policies\microsoft\mui\settings
  Opens key:              HKLM\software\policies\microsoft\mui\settings
  Opens key:              HKCU\
  Opens key:              HKCU\control panel\desktop\muicached\machinelanguageconfiguration
  Opens key:              HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
  Opens key:              HKCU\software\policies\microsoft\control panel\desktop
  Opens key:              HKCU\control panel\desktop\languageconfiguration
  Opens key:              HKCU\control panel\desktop
  Opens key:              HKCU\control panel\desktop\muicached
  Opens key:              HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
  Opens key:              HKLM\system\currentcontrolset\control\nls\sorting\versions
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
  Opens key:              HKCU\software\microsoft\windows nt\currentversion\appcompatflags
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:              HKLM\system\currentcontrolset\control\session manager
  Opens key:              HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
  Opens key:              HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
  Opens key:              HKLM\system\currentcontrolset\control\lsa
  Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
  Opens key:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
  Opens key:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32
  Opens key:              HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
  Opens key:              HKLM\
  Opens key:              HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
  Opens key:              HKLM\software\wow6432node\microsoft\ole
  Opens key:              HKLM\software\wow6432node\microsoft\ole\tracing
  Opens key:              HKLM\software\microsoft\ole\tracing
  Opens key:              HKLM\software\wow6432node\microsoft\oleaut
  Opens key:              HKCU\software\classes\
  Opens key:                HKCU\software\classes\wow6432node\clsid
  Opens key:                HKCR\wow6432node\clsid
  Opens key:                HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:                HKLM\software\microsoft\sqmclient\windows
  Opens key:                HKCU\software\microsoft\direct3d\shims\enableoverlays
  Opens key:                HKLM\software\wow6432node\microsoft\rpc
  Opens key:                HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:                HKLM\system\setup
  Opens key:                HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                HKLM\hardware\devicemap\video
  Opens key:                HKLM\system\currentcontrolset\control\video\{bf735b18-1b5a-4e14-b64c-
f2223c917d28}\0000
  Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_80ee&dev_beef&subsys_00000000&rev_00\3&267a616a&1&10
  Opens key:                HKLM\software\wow6432node\microsoft\directdraw\compatibility
  Opens key:                HKLM\software\wow6432node\microsoft\directdraw\compatibility\bug!
  Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\demolitionderby2
  Opens key:                HKLM\software\wow6432node\microsoft\directdraw\compatibility\diablo
  Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\mortalkombat3
  Opens key:                HKLM\software\wow6432node\microsoft\directdraw\compatibility\msgolf98
  Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nhlpowerplay
  Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nortonsysteminfo
  Opens key:                HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue
squadron
  Opens key:                HKLM\software\wow6432node\microsoft\directdraw\compatibility\savage
  Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\scorchedplanet
  Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\silentthunder
  Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft100
  Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft115
  Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraftdemo
  Opens key:                HKLM\software\wow6432node\microsoft\directdraw\compatibility\terracide
  Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\thirddimension
  Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark
  Opens key:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark
  Opens key:                HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:                HKLM\system\currentcontrolset\control\nls\sorting\ids
  Opens key:                HKLM\software\wow6432node\microsoft\directdraw\gammacalibrator
  Opens key:                HKLM\software\wow6432node\microsoft\directdraw
  Opens key:                HKLM\software\wow6432node\microsoft\direct3d
  Opens key:                HKLM\system\currentcontrolset\control\graphicsdrivers\scheduler
  Opens key:                HKCU\software\microsoft\windows\currentversion\directmanipulation
  Opens key:                HKLM\software\microsoft\com3
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{636b9f10-0c7d-11d1-95b2-
0020afdc7421}
  Opens key:                HKCR\activatableclasses\clsid
  Opens key:                HKCR\activatableclasses\clsid\{636b9f10-0c7d-11d1-95b2-0020afdc7421}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{636b9f10-0c7d-11d1-95b2-
0020afdc7421}
  Opens key:                HKCR\wow6432node\clsid\{636b9f10-0c7d-11d1-95b2-0020afdc7421}
```

```
  Opens key:                HKCU\software\classes\wow6432node\clsid\{636b9f10-0c7d-11d1-95b2-
0020afdc7421}\treatas
  Opens key:                HKCR\wow6432node\clsid\{636b9f10-0c7d-11d1-95b2-0020afdc7421}\treatas
  Opens key:                HKCU\software\classes\wow6432node\clsid\{636b9f10-0c7d-11d1-95b2-
0020afdc7421}\inprocserver32
  Opens key:                HKCR\wow6432node\clsid\{636b9f10-0c7d-11d1-95b2-
0020afdc7421}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{636b9f10-0c7d-11d1-95b2-
0020afdc7421}\inprochandler32
  Opens key:                HKCR\wow6432node\clsid\{636b9f10-0c7d-11d1-95b2-
0020afdc7421}\inprochandler32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{636b9f10-0c7d-11d1-95b2-
0020afdc7421}\inprochandler
  Opens key:                HKCR\wow6432node\clsid\{636b9f10-0c7d-11d1-95b2-
0020afdc7421}\inprochandler
  Opens key:                HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\setup
  Opens key:                HKLM\software\microsoft\windows\currentversion\setup
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion
  Opens key:                HKLM\system\currentcontrolset\control\deviceclasses\{6994ad04-93ef-11d0-
a3cc-00a0c9223196}
  Opens key:                HKLM\system\currentcontrolset\services\crypt32
  Opens key:                HKLM\software\wow6432node\microsoft\windows nt\currentversion\msasn1
  Opens key:                HKLM\software\wow6432node\microsoft\directmusic\defaults
  Opens key:                HKLM\software\wow6432node\microsoft\directmusic
  Opens key:                HKCU\software
  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\software\wow6432node\microsoft\ctf\compatibility\90d0d029326bfb8fd9a1a94749386ca7.exe
  Opens key:                HKLM\software\wow6432node\microsoft\ctf\
  Opens key:                HKLM\software\wow6432node\microsoft\ctf\knownclasses
  Opens key:                HKLM\system\currentcontrolset\control\sqmservicelist
  Opens key:                HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32
  Opens key:
HKCU\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
  Opens key:                HKLM\software\microsoft\windows\currentversion\mmdevices\audio\render\
  Opens key:                HKLM\software\microsoft\windows\currentversion\mmdevices\audio\capture\
  Opens key:
HKLM\system\currentcontrolset\control\mediaresources\directsound\application
compatibility\90d0d029326bfb8fd9a1a94749386ca7.exe436f524400092eb8\
  Opens key:
HKLM\system\currentcontrolset\control\mediaresources\directsound\application
compatibility\90d0d029326bfb8fd9a1a94749386ca7.exe436f524400092eb8
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}
  Opens key:                HKCR\activatableclasses\clsid\{bcde0395-e52f-467c-8e3d-c4579291692e}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}
  Opens key:                HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-c4579291692e}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}\treatas
  Opens key:                HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-c4579291692e}\treatas
  Opens key:                HKCU\software\classes\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}\inprocserver32
  Opens key:                HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}\inprochandler32
  Opens key:                HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}\inprochandler32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}\inprochandler
  Opens key:                HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}\inprochandler
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\segoe ui
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer
  Opens key:                HKLM\software\microsoft\windows\currentversion\policies\explorer
  Opens key:                HKCU\software\microsoft\windows\currentversion\policies\explorer
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[empty]
  Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
  Queries value:            HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
  Queries value:            HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
  Queries value:            HKCU\control panel\desktop[preferreduilanguages]
  Queries value:            HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\versions[]
  Queries value:            HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
  Queries value:            HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[90d0d029326bfb8fd9a1a94749386ca7.exe]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries value:            HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[90d0d029326bfb8fd9a1a94749386ca7]
  Queries value:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:            HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:            HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:            HKLM\software\microsoft\ole[aggressivemtatesting]
  Queries value:            HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:            HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:            HKLM\system\setup[oobeinprogress]
  Queries value:            HKLM\system\setup[systemsetupinprogress]
  Queries value:            HKLM\software\microsoft\rpc[idletimerwindow]
  Queries value:            HKLM\hardware\devicemap\video[maxobjectnumber]
  Queries value:            HKLM\hardware\devicemap\video[\device\video0]
  Queries value:            HKLM\system\currentcontrolset\control\class\{4d36e968-e325-11ce-bfc1-
08002be10318}\0000[pruningmode]
  Queries value:            HKLM\software\wow6432node\microsoft\directdraw\compatibility\bug![name]
  Queries value:            HKLM\software\wow6432node\microsoft\directdraw\compatibility\bug![flags]
  Queries value:            HKLM\software\wow6432node\microsoft\directdraw\compatibility\bug![id]
  Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\demolitionderby2[name]
```

```
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\demolitionderby2[flags]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\demolitionderby2[id]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\diablo[name]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\diablo[flags]
   Queries value:            HKLM\software\wow6432node\microsoft\directdraw\compatibility\diablo[id]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\mortalkombat3[name]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\mortalkombat3[flags]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\mortalkombat3[id]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\msgolf98[name]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\msgolf98[flags]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\msgolf98[id]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nhlpowerplay[name]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nhlpowerplay[flags]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nhlpowerplay[id]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nortonsysteminfo[name]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nortonsysteminfo[flags]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nortonsysteminfo[id]
   Queries value:            HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue
squadron[name]
   Queries value:            HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue
squadron[flags]
   Queries value:            HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue
squadron[id]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\savage[name]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\savage[flags]
   Queries value:            HKLM\software\wow6432node\microsoft\directdraw\compatibility\savage[id]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\scorchedplanet[name]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\scorchedplanet[flags]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\scorchedplanet[id]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\silentthunder[name]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\silentthunder[flags]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\silentthunder[id]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft100[name]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft100[flags]
   Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft100[id]
   Queries value:
```

```
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft115[name]
  Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft115[flags]
  Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft115[id]
  Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraftdemo[name]
  Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraftdemo[flags]
  Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraftdemo[id]
  Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\terracide[name]
  Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\terracide[flags]
  Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\terracide[id]
  Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\thirddimension[name]
  Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\thirddimension[flags]
  Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\thirddimension[id]
  Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[name]
  Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[flags]
  Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[id]
  Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[name]
  Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[flags]
  Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[id]
  Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Queries value:          HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
  Queries value:          HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
  Queries value:          HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
  Queries value:          HKLM\software\wow6432node\microsoft\directdraw[modexonly]
  Queries value:          HKLM\software\wow6432node\microsoft\directdraw[emulationonly]
  Queries value:          HKLM\software\wow6432node\microsoft\directdraw[showframerate]
  Queries value:          HKLM\software\wow6432node\microsoft\directdraw[enableprintscreen]
  Queries value:          HKLM\software\wow6432node\microsoft\directdraw[forceagpsupport]
  Queries value:          HKLM\software\wow6432node\microsoft\directdraw[disableagpsupport]
  Queries value:          HKLM\software\wow6432node\microsoft\directdraw[disablemmx]
  Queries value:          HKLM\software\wow6432node\microsoft\directdraw[disableddscapsinddsd]
  Queries value:          HKLM\software\wow6432node\microsoft\directdraw[disablewidersurfaces]
  Queries value:          HKLM\software\wow6432node\microsoft\directdraw[usenonlocalvidmem]
  Queries value:          HKLM\software\wow6432node\microsoft\directdraw[forcerefreshrate]
  Queries value:          HKLM\software\wow6432node\microsoft\direct3d[flipnovsync]
  Queries value:          HKLM\software\wow6432node\microsoft\direct3d[minimumlocalvidmem]
  Queries value:          HKLM\software\microsoft\com3[com+enabled]
  Queries value:          HKCR\wow6432node\clsid\{636b9f10-0c7d-11d1-95b2-0020afdc7421}[]
  Queries value:          HKCR\wow6432node\clsid\{636b9f10-0c7d-11d1-95b2-
0020afdc7421}\inprocserver32[inprocserver32]
  Queries value:          HKCR\wow6432node\clsid\{636b9f10-0c7d-11d1-95b2-
0020afdc7421}\inprocserver32[]
  Queries value:          HKCR\wow6432node\clsid\{636b9f10-0c7d-11d1-95b2-
0020afdc7421}\inprocserver32[threadingmodel]
  Queries value:          HKLM\software\microsoft\ole[maxsxshashcount]
  Queries value:          HKLM\system\currentcontrolset\control\wmi\security[12e1ddac-7ebb-434f-
bc58-54c27d745f8f]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
  Queries value:              HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
  Queries value:              HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
  Queries value:              HKLM\software\wow6432node\microsoft\directmusic[defaulttomskernelsynth]
  Queries value:              HKLM\software\wow6432node\microsoft\directmusic[disablehwacceleration]
  Queries value:              HKLM\software\wow6432node\microsoft\direct3d[disablemmx]
  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\system\currentcontrolset\control\nls\locale[00000409]
  Queries value:              HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:              HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
  Queries value:              HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave1]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave2]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave3]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave4]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave5]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave6]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave7]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave8]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave9]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi1]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi2]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi3]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi4]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi5]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi6]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi7]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi8]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi9]
  Queries value:
HKCU\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
  Queries value:              HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-c4579291692e}[]
```

```
   Queries value:               HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}\inprocserver32[inprocserver32]
   Queries value:               HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}\inprocserver32[]
   Queries value:               HKCR\wow6432node\clsid\{bcde0395-e52f-467c-8e3d-
c4579291692e}\inprocserver32[threadingmodel]
   Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
   Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
   Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
   Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
   Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
   Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
   Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
   Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
   Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
   Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
   Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
   Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
   Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
   Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
   Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
   Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
   Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
   Queries value:               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
   Sets/Creates value:          HKLM\software\wow6432node\microsoft\direct3d\mostrecentapplication[name]
   Value changes:
HKLM\software\wow6432node\microsoft\directdraw\mostrecentapplication[name]
   Value changes:               HKLM\software\wow6432node\microsoft\directdraw\mostrecentapplication[id]
```