Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 77, Task ID: 308

Task ID:	308
Risk Level:	4
Date Processed:	2016-04-28 12:55:43 (UTC)
Processing Time:	61.15 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\ca293fc948db9309896d46f093b9ca26.exe"

Sample ID:	77
Type:	basic
Owner:	admin
Label:	ca293fc948db9309896d46f093b9ca26
Date Added:	2016-04-28 12:44:57 (UTC)
File Type:	PE32:win32:gui
File Size:	103008 bytes
MD5:	ca293fc948db9309896d46f093b9ca26
SHA256:	71d9958e04ef992e1b465094a4009364328284b5f81488c5c6dc0d24d216dc60
Description:	None

Pattern Matching Results

4 Reads process memory

Process/Thread Events

Creates process:	C:\windows\temp\ca293fc948db9309896d46f093b9ca26.exe ["C:\windows\temp\ca293fc948db9309896d46f093b9ca26.exe"]
Reads from process:	PID:1216 C:\Windows\System32\dwm.exe
Reads from process:	PID:1240 C:\Windows\explorer.exe
Reads from process:	PID:1312 C:\Windows\System32\taskhost.exe
Reads from process:	PID:1444 C:\Program Files\Adobe\Reader 9.0\Reader\reader_sl.exe
Reads from process:	PID:1452 C:\Windows\System32\mobsync.exe
Reads from process:	PID:2172 C:\Windows\System32\conhost.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex:	\Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1

File System Events

Opens:	C:\Windows\Prefetch\CA293FC948DB9309896D46F093B9C-E972BB19.pf
Opens:	C:\Windows\System32
Opens:	C:\windows\temp\ca293fc948db9309896d46f093b9ca26.exe.Local\
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
Opens:	C:\windows\temp\VERSION.dll
Opens:	C:\Windows\System32\version.dll
Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\Windows\WindowsShell.Manifest
Opens:	C:\windows\temp\ca293fc948db9309896d46f093b9ca26_lng.ini
Opens:	C:\Windows\System32\uxtheme.dll
Opens:	C:\windows\temp\dwmapi.dll
Opens:	C:\Windows\System32\dwmapi.dll
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\Windows\Fonts\StaticCache.dat

```
  Opens:                    C:\Windows\System32\en-US\user32.dll.mui
  Opens:                    C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                    C:\Windows\system32\uxtheme.dll.Config
  Opens:                    C:\windows\temp\ca293fc948db9309896d46f093b9ca26.cfg
  Opens:                    C:\Windows\System32\ole32.dll
  Opens:                    C:\Windows\System32\rpcss.dll
  Opens:                    C:\windows\temp\CRYPTBASE.dll
  Opens:                    C:\Windows\System32\cryptbase.dll
  Opens:                    C:\Windows\Temp
  Opens:                    C:\Windows\Fonts\arialbd.ttf
  Opens:                    C:\Windows\System32\vga.dll
  Opens:                    C:\Windows\System32\vga256.dll
  Opens:                    C:\Windows\System32\vga64k.dll
  Opens:                    C:\Windows\System32\rdpdd.dll
  Opens:                    C:\Windows\System32\RDPENCDD.dll
  Opens:                    C:\Windows\System32\RDPREFDD.dll
  Opens:                    C:\Windows\explorer.exe
  Opens:                    C:\Windows\en-US\explorer.exe.mui
  Opens:                    C:\Windows\System32\calc.exe
  Reads from:               C:\Windows\Fonts\StaticCache.dat
```

Windows Registry Events

```
  Creates key:              HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-
08002be10318}\0000
  Opens key:                HKLM\system\currentcontrolset\control\session manager
  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\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKCU\
  Opens key:                HKCU\control panel\desktop\muicached\machinelanguageconfiguration
  Opens key:                HKLM\software\policies\microsoft\mui\settings
  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\microsoft\windows\currentversion\sidebyside
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:                HKLM\system\currentcontrolset\control\nls\sorting\versions
  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\
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\windows
  Opens key:                HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:                HKLM\system\currentcontrolset\control\nls\extendedlocale
  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\microsoft\windows nt\currentversion\diagnostics
  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\system\currentcontrolset\control\cmf\config
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
  Opens key:                HKLM\software\microsoft\windows\windows error reporting\wmr
  Opens key:                HKLM\software\microsoft\windows\currentversion\policies\explorer
  Opens key:                HKCU\software\microsoft\windows\currentversion\policies\explorer
  Opens key:
HKLM\software\microsoft\ctf\compatibility\ca293fc948db9309896d46f093b9ca26.exe
  Opens key:                HKLM\software\microsoft\ole
  Opens key:                HKLM\software\microsoft\ole\tracing
  Opens key:                HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
  Opens key:                HKLM\software\microsoft\ctf\
  Opens key:                HKLM\software\microsoft\ctf\knownclasses
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\arial
  Opens key:                HKLM\hardware\devicemap\video
  Opens key:                HKLM\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000
  Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_80ee&dev_beef&subsys_00000000&rev_00\3&267a616a&0&10
  Opens key:
HKLM\system\currentcontrolset\enum\display\default_monitor\4&2abfaa30&0&12345678&00&02
  Opens key:                HKLM\system\currentcontrolset\hardware
profiles\current\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000
  Opens key:                HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-fd27e3774e32}\0000
  Opens key:                HKLM\system\currentcontrolset\control\watchdog\display
  Opens key:                HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-
08002be10318}\0000\modes
  Opens key:                HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-
08002be10318}\0000\modes\640,480
  Opens key:
HKLM\system\currentcontrolset\enum\display\default_monitor\4&2abfaa30&0&12345678&00&02\device
parameters
  Opens key:                HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
9dd4432fa2e9}\0000
  Opens key:                HKLM\system\currentcontrolset\hardware
profiles\current\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
9dd4432fa2e9}\0000
  Opens key:                HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000
  Opens key:                HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000
  Opens key:                HKLM\system\currentcontrolset\hardware
profiles\current\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000
  Opens key:                HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-0d8e74595f78}\0000
  Opens key:                HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
8ed0c8eb59a8}\0000
  Opens key:                HKLM\system\currentcontrolset\hardware
profiles\current\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
8ed0c8eb59a8}\0000
  Opens key:                HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-8ed0c8eb59a8}\0000
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
  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:            HKCU\control panel\desktop[preferreduilanguages]
  Queries value:            HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Queries value:              HKLM\system\currentcontrolset\control\nls\sorting\versions[]
  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[ca293fc948db9309896d46f093b9ca26]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  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\locale[00000409]
  Queries value:              HKLM\system\currentcontrolset\control\nls\language groups[1]
  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\system\currentcontrolset\control\cmf\config[system]
  Queries value:              HKCU\control panel\desktop[smoothscroll]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewalphaselect]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[acclistviewv6]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe
```

```
ui]
  Queries value:              HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
  Queries value:              HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:              HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:              HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
  Queries value:              HKLM\software\microsoft\ctf[enableanchorcontext]
  Queries value:              HKLM\hardware\devicemap\video[maxobjectnumber]
  Queries value:              HKLM\hardware\devicemap\video[\device\video3]
  Queries value:              HKLM\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000[pruningmode]
  Queries value:
HKLM\system\currentcontrolset\enum\display\default_monitor\4&2abfaa30&0&12345678&00&02[devicedesc]
  Queries value:
HKLM\system\currentcontrolset\enum\display\default_monitor\4&2abfaa30&0&12345678&00&02[hardwareid]
  Queries value:
HKLM\system\currentcontrolset\enum\display\default_monitor\4&2abfaa30&0&12345678&00&02[driver]
  Queries value:              HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000[defaultsettings.bitsperpel]
  Queries value:              HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000[defaultsettings.xresolution]
  Queries value:              HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000[defaultsettings.yresolution]
  Queries value:              HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000[defaultsettings.vrefresh]
  Queries value:              HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000[defaultsettings.flags]
  Queries value:              HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000[defaultsettings.xpanning]
  Queries value:              HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000[defaultsettings.ypanning]
  Queries value:              HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000[defaultsettings.orientation]
  Queries value:              HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000[defaultsettings.fixedoutput]
  Queries value:              HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000[attach.relativex]
  Queries value:              HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000[attach.relativey]
  Queries value:              HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000[attach.todesktop]
  Queries value:              HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000[defaultsettings.driverextra]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-
08002be10318}\0000\modes\640,480[mode1]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-
08002be10318}\0000\modes\640,480[mode2]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-
08002be10318}\0000\modes\640,480[mode3]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-
```

```
08002be10318}\0000\modes\640,480[mode4]
  Queries value:               HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-
08002be10318}\0000\modes\640,480[mode5]
  Queries value:               HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-
08002be10318}\0000\modes\640,480[mode6]
  Queries value:               HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-
08002be10318}\0000\modes\640,480[mode7]
  Queries value:               HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-
08002be10318}\0000\modes\640,480[mode8]
  Queries value:               HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-
08002be10318}\0000\modes\640,480[mode9]
  Queries value:
HKLM\system\currentcontrolset\enum\display\default_monitor\4&2abfaa30&0&12345678&00&02\device
parameters[edid]
  Queries value:               HKLM\hardware\devicemap\video[\device\video0]
  Queries value:               HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
9dd4432fa2e9}\0000[pruningmode]
  Queries value:               HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
9dd4432fa2e9}\0000[defaultsettings.bitsperpel]
  Queries value:               HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
9dd4432fa2e9}\0000[defaultsettings.xresolution]
  Queries value:               HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
9dd4432fa2e9}\0000[defaultsettings.yresolution]
  Queries value:               HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
9dd4432fa2e9}\0000[defaultsettings.vrefresh]
  Queries value:               HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
9dd4432fa2e9}\0000[defaultsettings.flags]
  Queries value:               HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
9dd4432fa2e9}\0000[defaultsettings.xpanning]
  Queries value:               HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
9dd4432fa2e9}\0000[defaultsettings.ypanning]
  Queries value:               HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
9dd4432fa2e9}\0000[defaultsettings.orientation]
  Queries value:               HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
9dd4432fa2e9}\0000[defaultsettings.fixedoutput]
  Queries value:               HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
9dd4432fa2e9}\0000[attach.relativex]
  Queries value:               HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
9dd4432fa2e9}\0000[attach.relativey]
  Queries value:               HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
9dd4432fa2e9}\0000[attach.todesktop]
  Queries value:               HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-
9dd4432fa2e9}\0000[defaultsettings.driverextra]
  Queries value:               HKLM\hardware\devicemap\video[\device\video1]
  Queries value:               HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000[pruningmode]
  Queries value:               HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000[defaultsettings.bitsperpel]
  Queries value:               HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000[defaultsettings.xresolution]
  Queries value:               HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000[defaultsettings.yresolution]
  Queries value:               HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000[defaultsettings.vrefresh]
  Queries value:               HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000[defaultsettings.flags]
  Queries value:               HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000[defaultsettings.xpanning]
  Queries value:               HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000[defaultsettings.ypanning]
  Queries value:               HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000[defaultsettings.orientation]
  Queries value:               HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
```

```
0d8e74595f78}\0000[defaultsettings.fixedoutput]
  Queries value:              HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000[attach.relativex]
  Queries value:              HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000[attach.relativey]
  Queries value:              HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000[attach.todesktop]
  Queries value:              HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-
0d8e74595f78}\0000[defaultsettings.driverextra]
  Queries value:              HKLM\hardware\devicemap\video[\device\video2]
  Queries value:              HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
8ed0c8eb59a8}\0000[pruningmode]
  Queries value:              HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
8ed0c8eb59a8}\0000[defaultsettings.bitsperpel]
  Queries value:              HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
8ed0c8eb59a8}\0000[defaultsettings.xresolution]
  Queries value:              HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
8ed0c8eb59a8}\0000[defaultsettings.yresolution]
  Queries value:              HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
8ed0c8eb59a8}\0000[defaultsettings.vrefresh]
  Queries value:              HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
8ed0c8eb59a8}\0000[defaultsettings.flags]
  Queries value:              HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
8ed0c8eb59a8}\0000[defaultsettings.xpanning]
  Queries value:              HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
8ed0c8eb59a8}\0000[defaultsettings.ypanning]
  Queries value:              HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
8ed0c8eb59a8}\0000[defaultsettings.orientation]
  Queries value:              HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
8ed0c8eb59a8}\0000[defaultsettings.fixedoutput]
  Queries value:              HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
8ed0c8eb59a8}\0000[attach.relativex]
  Queries value:              HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
8ed0c8eb59a8}\0000[attach.relativey]
  Queries value:              HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
8ed0c8eb59a8}\0000[attach.todesktop]
  Queries value:              HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-
8ed0c8eb59a8}\0000[defaultsettings.driverextra]
  Queries value:              HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
```