Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 77, Task ID: 306

Task ID:	306
Risk Level:	4
Date Processed:	2016-04-28 12:55:39 (UTC)
Processing Time:	61.14 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:2040 C:\Windows\System32\taskhostex.exe
Reads from process: PID:1608 C:\Windows\explorer.exe
Reads from process: PID:2448 C:\Program Files (x86)\Adobe\Reader 9.0\Reader\reader_sl.exe
Reads from process: PID:2860 C:\Windows\System32\conhost.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens: C:\Windows\Prefetch\CA293FC948DB9309896D46F093B9C-E972BB19.pf
Opens: C:\Windows
Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\SysWOW64
Opens: C:\Windows\SysWOW64\apphelp.dll
Opens: C:\Windows\Temp\ca293fc948db9309896d46f093b9ca26.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\version.dll
Opens: C:\Windows\SysWOW64\combase.dll
Opens: C:\Windows\SysWOW64\SHCore.dll
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\Windows\SysWOW64\msvcrt.dll
Opens: C:\Windows\SysWOW64\user32.dll
Opens: C:\Windows\SysWOW64\gdi32.dll
Opens: C:\Windows\SysWOW64\shlwapi.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\shell32.dll
Opens: C:\Windows\SysWOW64\comdlg32.dll
Opens: C:\Windows\SysWOW64\imm32.dll
Opens: C:\Windows\SysWOW64\msctf.dll
Opens: C:\Windows\WindowsShell.Manifest
Opens: C:\Windows\SysWOW64\uxtheme.dll
Opens: C:\Windows\SysWOW64\dwmapi.dll
Opens: C:\Windows\Fonts\StaticCache.dat
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\SysWOW64\uxtheme.dll.Config
Opens: C:\windows\temp\ca293fc948db9309896d46f093b9ca26.cfg
Opens: C:\Windows\SysWOW64\ole32.dll
Opens: C:\Windows\SysWOW64\oleaut32.dll
Opens: C:\Windows\Fonts\arialbd.ttf
Opens: C:\Windows\SysWOW64\psapi.dll
Opens: C:\Windows\SysWOW64\calc.exe
Reads from: C:\Windows\Fonts\StaticCache.dat

Windows Registry Events

Creates key: HKLM\system\currentcontrolset\control\graphicsdrivers\connectivity\
Creates key: HKLM\system\currentcontrolset\control\graphicsdrivers\connectivity
Creates key: HKLM\system\currentcontrolset\control\graphicsdrivers\connectivity\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14
Creates key: HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\
Creates key: HKLM\system\currentcontrolset\control\graphicsdrivers\configuration
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\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\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\ole
Opens key: HKLM\software\wow6432node\microsoft\ole\tracing
Opens key: HKLM\software\microsoft\ole\tracing
Opens key: HKLM\software\policies\microsoft\sqmclient\windows
Opens key: HKLM\software\microsoft\sqmclient\windows
Opens key: HKCU\software\microsoft\windows\currentversion\directmanipulation
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\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: HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\fontsubstitutes
Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids
Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
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
Opens key:
HKLM\software\wow6432node\microsoft\ctf\compatibility\ca293fc948db9309896d46f093b9ca26.exe
Opens key: HKLM\software\wow6432node\microsoft\ctf\
Opens key: HKLM\software\wow6432node\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\{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\system\currentcontrolset\enum\display\default_monitor\4&39fc21a1&0&uid0
Opens key:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_1414_008d_ffffffff_ffffffff_0^cc77560bc3634a486857716562968286
Opens key:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14
Opens key:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_ryi0001 agnieszka
01_1d_07d7_b2_1414_008d_ffffffff_ffffffff_0^700ef59a5da31cbd79f31237af2ad4c4
Opens key:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msh062e0_00_07db_c6^182fdc0875f0a76803e4a9848a8c1ea7
Opens key:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00
Opens key:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-
08002be10318}\0001
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-
08002be10318}\0001\modes
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-
08002be10318}\0001\modes\640,480
Opens key:
HKLM\system\currentcontrolset\enum\display\default_monitor\4&39fc21a1&0&uid0\device parameters
Opens key: HKLM\system\currentcontrolset\hardware
profiles\unitedvideo\control\video\{bf735b18-1b5a-4e14-b64c-f2223c917d28}\0000
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[ca293fc948db9309896d46f093b9ca26.exe]
Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[ca293fc948db9309896d46f093b9ca26]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
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\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: 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\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\windows\windows error reporting\wmr[disable]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
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\system\currentcontrolset\enum\display\default_monitor\4&39fc21a1&0&uid0[devicedesc]
Queries value: HKLM\system\currentcontrolset\enum\display\default_monitor\4&39fc21a1&0&uid0[hardwareid]
Queries value: HKLM\system\currentcontrolset\enum\display\default_monitor\4&39fc21a1&0&uid0[driver]
Queries value: HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_1414_008d_ffffffff_ffffffff_0^cc77560bc3634a486857716562968286[timestamp]
Queries value: HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_1414_008d_ffffffff_ffffffff_0^cc77560bc3634a486857716562968286[setid]
Queries value: HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14[timestamp]
Queries value: HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14[setid]
Queries value: HKLM\system\currentcontrolset\control\graphicsdrivers\connectivity\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14[recent]
Queries value: HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_ryi0001 agnieszka 01_1d_07d7_b2_1414_008d_ffffffff_ffffffff_0^700ef59a5da31cbd79f31237af2ad4c4[timestamp]
Queries value: HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msh062e0_00_07db_c6^182fdc0875f0a76803e4a9848a8c1ea7[timestamp]
Queries value: HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00[primsurfsize.cx]
Queries value: HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00[primsurfsize.cy]
Queries value: HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00[stride]
Queries value:

HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00[pixelformat]
Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00[colorbasis]
Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00[position.cx]
Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00[position.cy]
Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[flags]
Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[videostandard]
Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[activesize.cx]
Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[activesize.cy]
Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[vsyncfreq.numerator]
Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[vsyncfreq.denominator]
Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[hsyncfreq.numerator]
Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[hsyncfreq.denominator]
Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[pixelrate]
Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[scanlineordering]
Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[scaling]
Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[rotation]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-08002be10318}\0001\modes\640,480[mode1]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-08002be10318}\0001\modes\640,480[mode2]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-08002be10318}\0001\modes\640,480[mode3]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-08002be10318}\0001\modes\640,480[mode4]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-08002be10318}\0001\modes\640,480[mode5]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-08002be10318}\0001\modes\640,480[mode6]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-08002be10318}\0001\modes\640,480[mode7]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-08002be10318}\0001\modes\640,480[mode8]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-08002be10318}\0001\modes\640,480[mode9]
Queries value:
HKLM\system\currentcontrolset\enum\display\default_monitor\4&39fc21a1&0&uid0\device parameters[edid]
Queries value: HKLM\system\currentcontrolset\hardware profiles\unitedvideo\control\video\{bf735b18-1b5a-4e14-b64c-f2223c917d28}\0000[defaultsettings.bitsperpel]
Queries value: HKLM\system\currentcontrolset\hardware profiles\unitedvideo\control\video\{bf735b18-1b5a-4e14-b64c-f2223c917d28}\0000[defaultsettings.xresolution]
Queries value: HKLM\system\currentcontrolset\hardware profiles\unitedvideo\control\video\{bf735b18-1b5a-4e14-b64c-f2223c917d28}\0000[defaultsettings.yresolution]
Queries value: HKLM\system\currentcontrolset\hardware profiles\unitedvideo\control\video\{bf735b18-1b5a-4e14-b64c-f2223c917d28}\0000[defaultsettings.vrefresh]
Queries value: HKLM\system\currentcontrolset\hardware profiles\unitedvideo\control\video\{bf735b18-1b5a-4e14-b64c-f2223c917d28}\0000[defaultsettings.flags]
Queries value: HKLM\system\currentcontrolset\hardware profiles\unitedvideo\control\video\{bf735b18-1b5a-4e14-b64c-f2223c917d28}\0000[defaultsettings.xpanning]
Queries value: HKLM\system\currentcontrolset\hardware profiles\unitedvideo\control\video\{bf735b18-1b5a-4e14-b64c-f2223c917d28}\0000[defaultsettings.ypanning]
Queries value: HKLM\system\currentcontrolset\hardware profiles\unitedvideo\control\video\{bf735b18-1b5a-4e14-b64c-f2223c917d28}\0000[defaultsettings.orientation]
Queries value: HKLM\system\currentcontrolset\hardware profiles\unitedvideo\control\video\{bf735b18-1b5a-4e14-b64c-f2223c917d28}\0000[defaultsettings.fixedoutput]
Queries value: HKLM\system\currentcontrolset\hardware profiles\unitedvideo\control\video\{bf735b18-1b5a-4e14-b64c-f2223c917d28}\0000[attach.relativex]
Queries value: HKLM\system\currentcontrolset\hardware profiles\unitedvideo\control\video\{bf735b18-1b5a-4e14-b64c-f2223c917d28}\0000[attach.relativey]
Queries value: HKLM\system\currentcontrolset\hardware profiles\unitedvideo\control\video\{bf735b18-1b5a-4e14-b64c-f2223c917d28}\0000[attach.todesktop]