Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID: 306 Risk Level:

2016-04-28 12:55:39 (UTC) Date Processed:

Processing Time: 61.14 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\ca293fc948db9309896d46f093b9ca26.exe"

Sample ID Type: basic Owner: admir

Label: ca293fc948db9309896d46f093b9ca26 Date Added 2016-04-28 12:44:57 (UTC)

PE32:win32:gui File Type: File Size

103008 bytes ca293fc948db9309896d46f093b9ca26 MD5:

SHA256: 71d9958e04ef992e1b465094a4009364328284b5f81488c5c6dc0d24d216dc60

Description:

Pattern Matching Results

4 Reads process memory

Process/Thread Events

Creates process: C:\windows\temp\ca293fc948db9309896d46f093b9ca26.exe

["C:\windows\temp\ca293fc948db9309896d46f093b9ca26.exe"]

PID:2040 C:\Windows\System32\taskhostex.exe

Reads from process: PID:1608 C:\Windows\explorer.exe PID:2486 C:\Program Files (x86)\Adobe\Reader 9.0\Reader\reader_sl.exe PID:2860 C:\Windows\System32\conhost.exe Reads from process:

Reads from process

Named Object Events

\Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

C:\Windows\Prefetch\CA293FC948DB9309896D46F093B9C-E972BB19.pf Opens C:\Windows

Opens \Windows\System32\wow64.dll Opens

C:\Windows\SysWOW64
C:\Windows\SysWOW64\apphelp.dll Opens

Opens:

C:\Windows\Temp\ca293fc948db9309896d46f093b9ca26.exe C:\Windows\SysWOW64\ntdll.dll Opens

Opens: C:\Windows\SysWOW64\kernel32.dll
C:\Windows\SysWOW64\KernelBase.dll Opens: Opens: :\Windows\apppatch\sysmain.sdb Opens:

 $Opens: C: \verb|Windows| WinSxS\\ \times 86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985$

C:\Windows\WinSxS\x86 microsoft.windows.commoncontrols_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll

Opens: C:\Windows\SvsWOW64\version.dll :\Windows\SysWOW64\combase.dll Opens: Opens: C:\Windows\SysWOW64\SHCore.dll
C:\Windows\SysWOW64\sechost.dll C:\Windows\SysWOW64\msvcrt.dll
C:\Windows\SysWOW64\user32.dll Opens: Opens Opens: C:\Windows\SysWOW64\gdi32.dll
C:\Windows\SysWOW64\shlwapi.dll Opens

C:\Windows\SysWOW64\bcryptprimitives.dll
C:\Windows\SysWOW64\cryptbase.dll Opens Opens: C:\Windows\SysWOW64\sspicli.dll C:\Windows\SysWOW64\rpcrt4.dll Opens Opens C:\Windows\SysWOW64\shell32.dll C:\Windows\SysWOW64\comdlg32.dll Opens: Opens: :\Windows\SysWOW64\imm32.dll C:\Windows\SysWOW64\msctf.dll Opens: Opens: \Windows\WindowsShell.Manifest Opens: C:\Windows\SysWOW64\uxtheme.dll Opens \Windows\SysWOW64\dwmapi.dll

C:\Windows\Fonts\StaticCache.dat \Windows\Globalization\Sorting\SortDefault.nls Opens C:\Windows\SysWOW64\uxtheme.dll.Config C:\windows\temp\ca293fc948db9309896d46f093b9ca26.cfg Opens:

Opens C:\Windows\SysWOW64\ole32.dll C:\Windows\SysWOW64\oleaut32.dll Opens: Opens:

C:\Windows\Fonts\arialbd.ttf
C:\Windows\SysWOW64\psapi.dll Opens: Opens C:\Windows\SysWOW64\calc.exe C:\Windows\Fonts\StaticCache.dat Reads from:

Windows Registry Events

Opens

Creates key: HKLM\system\currentcontrolset\control\graphicsdrivers\connectivity Creates key: ${\tt HKLM \ } system \verb|\ control \ graphics drivers \verb|\ connectivity| \\$

Creates key

HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\ Creates key

Creates key $\label{thm:hklm} HKLM \system \configuration \ HKLM \system \system \system \system \system \system \ HKLM \system \system \system \system \system \system \system \ HKLM \system \s$

Opens key: Opens key: ${\tt HKLM \ } system \verb|\ current control \verb|\ terminal server|$ HKLM\svstem\currentcontrolset\control\safeboot\option Opens key Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll Opens key

HKLM\softwar e\wow6432node\policies\microsoft\windows\safer\codeidentifiers

Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers Opens key HKLM\system\currentcontrolset\control\nls\customlocale HKLM\system\currentcontrolset\control\nls\language Opens key: Opens key: Opens key: Opens key: Opens key: $\label{thm:local-policies} HKLM\software\wow6432node\policies\microsoft\mui\settings$

Opens key ${\it HKLM \backslash software \backslash policies \backslash \dot microsoft \backslash mui \backslash settings}$

Opens key

Opens key HKCU\control panel\desktop\muicached\machinelanguageconfiguration

```
HKLM\svstem\currentcontrolset\control\mui\settings\languageconfiguration
   Opens key
                                                      HKCU\software\policies\microsoft\control panel\desktop
    Opens key:
                                                      \label{thm:local_hamilton} \begin{tabular}{ll} HKCU \control panel \desktop \label{thm:local_hamilton} \end{tabular} AKCU \control panel \desktop \label{tabular}
   Opens key
    Opens key:
   Opens key
                                                      \label{thm:local-ham} HKCU\control\ panel\desktop\muicached \\ HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside \\
   Opens key
   Opens key:
Opens key:
                                                      \label{thm:local} HKLM \system \current control system \current control system \current versions \\ HKLM \system \current version \app compatflags \dbglog \\
   Opens key
                                                      HKCU\software\microsoft\windows nt\currentversion\appcompatflags
                                                      HKLM\software\microsoft\windows
   Opens key
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
                                                      HKLM\software\wow6432node\microsoft\windows
   Opens key:
nt\currentversion\compatibility32
   Opens key:
                                                      HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
   Opens key:
    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
HKLMNsystem\currentcontrolset\policies\microsoft\cryptography\configuration Opens key: HKLM\software\wow6432node\microsoft\ole
    Opens key:
                                                      HKLM \verb|\software\\| wow 6432 node\\| 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\svstem\currentcontrolset\control\nls\extendedlocale
                                                      HKLM\system\currentcontrolset\control\nls\locale
    Opens key:
   Opens key
                                                      HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
                                                      HKLM\system\currentvorsoft\windows nt\currentversion\fontlink\systemlink
   Opens key:
   Opens key
   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
                                                      HKCU\software\microsoft\windows\currentversion\explorer\advanced
   Opens key:
    Opens key:
                                                      HKLM\software\wow6432node\microsoft\windows
nt\currentversion\fontsubstitutes
   Opens key:
                                                      HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
                                                      HKLM\svstem\currentcontrolset\control\nls\sorting\ids
   Opens kev:
                                                      HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
    Opens key:
   Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explored in the property of the propert
   Opens kev:
                                                      HKLM\software\microsoft\windows\currentversion\policies\explorer
                                                      HKCU\software\microsoft\windows\currentversion\policies\explorer
   Opens key:
   Opens key
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus ctf \setminus compatibility \setminus ca293fc 948 db 9309896d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 9309896d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 9309896d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 9309896d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 9309896d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 9309896d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 9309896d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 9309896d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 9309896d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 9309896d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 9309896d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 9309896d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 9309896d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 9309896d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 9309896d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 9309896d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 9309896d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 9309896d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 930986d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 930986d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 930986d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 930986d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 930986d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 930986d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 930986d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 930986d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 930986d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 930986d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 930986d46f0 93b9 ca26.exe + compatibility \setminus ca293fc 948 db 930986d46f0 93b9 ca26.exe + compatibility \setminus ca295fc 948 db 930986d46f0 93b9 ca26.exe + compatibility \setminus ca295fc 948 db 930986d46f0 948 db 930986d66f0 948 db 
   Opens key:
                                                     HKLM\software\wow6432node\microsoft\ctf\
HKLM\software\wow6432node\microsoft\ctf\knownclasses
   Opens key:
   Opens key:
                                                      HKLM\software\microsoft\window
nt\currentversion\languagepack\surrogatefallback\arial
   Opens key:
                                                      HKLM\hardware\devicemap\video
                                                      HKLM\system\currentcontrolset\control\video\{bf735b18-1b5a-4e14-b64c-
   Opens key
f2223c917d28}\0000
   Opens kev:
Opens kev:
HKLM\system\currentcontrolset\enum\display\default_monitor\4&39fc21a1&0&uid0
   Opens kev:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_1414_008d_ffffffffffffff_0^cc77560bc3634a486857716562968286
   Opens key:
Opens key: HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_ryi0001 agnieszka
01_1d_07d7_b2_1414_008d_ffffffffffffffff0^700ef59a5da31cbd79f31237af2ad4c4
Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_0020000_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
                                                      HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-
   Opens key
08002be10318}\0001\modes\640,480
   Opens key:
HKLM \setminus system \setminus current control set \vdash mum \mid display \mid default\_monitor \mid 4\&39fc21a1\&0\&uid0 \mid device parameters \mid default\_monitor \mid device parameters \mid default\_monitor \mid default\_monitor \mid device parameters \mid default\_monitor \mid default\_monitor \mid device parameters \mid default\_monitor \mid 
Opens key: HKLM\system\urrentcontrolset\hardware profiles\unitedvideo\control\video\{bf735b18-1b5a-4e14-b64c-f2223c917d28}\0000
   Queries value:
Queries value:
                                                      Queries value:
\label{lem:hklm} \begin{tabular}{ll} HKLM \software \verb|\policies|microsoft| windows \safer \code identifiers [transparent enabled] \end{tabular}
   Queries value:
                                                      HKLM\system\currentcontrolset\control\nls\customlocale[empty]
    Queries value:
HKLM\svstem\currentcontrolset\control\mui\uilanguages\en-usftvpel
   Oueries value:
    Queries value:
                                                      HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
    Queries value:
                                                      HKCU\control panel\desktop[preferreduilanguages]
   Oueries value:
                                                      HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
    Queries value:
HKLM\system\currentcontrolset\control\nls\sorting\versions[]
   Queries value:
   Queries value
                                                      HKCU\software\microsoft\windows
```

nt\currentversion\appcompatflags[showdebuginfo]

```
Queries value:
                                                     HKLM\system\currentcontrolset\control\session manager[safed]]searchmodel
                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
                                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
   Oueries value
\begin{tabular}{ll} options $$ \dlnx options [ca293fc948db9309896d46f093b9ca26.exe] \\ Queries value: $$ HKLM \software \microsoft \windows $$ \end{tabular}
\label{lem:ntcurrent} $$ ntcurrentversion\gre\_initialize[disablemetafiles] $$ Queries value: $$ HKLM\software\wow6432node\microsoft\windows $$ $$ $$ $$
nt\currentversion\compatibility32[ca293fc948db9309896d46f093b9ca26]
                                                     HKLM\software\wow6432node\microsoft\windows
   Queries value
nt\currentversion\windows[loadappinit_dlls]
                                                     HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
   Queries value:
                                                     HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy] HKLM\software\microsoft\ole[pageallocatorusesystemheap]
    Queries value:
    Queries value:
    Queries value:
                                                      HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
                                                     HKLM\software\microsoft\ole[aggressivemtatesting]
   Queries value:
    Queries value:
                                                      HKLM\software\microsoft\sqmclient\windows[ceipenable]
    Oueries value:
                                                     HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
                                                      HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
    Queries value
   Queries value:
                                                     HKLM\system\currentcontrolset\control\nls\locale[00000409]
                                                      HKLM\system\currentcontrolset\control\nls\language groups[1]
    Queries value:
   Oueries value
                                                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
   Oueries value
                                                     HKI M\software\microsoft\window
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane1]
   Oueries value
                                                     HKLM\software\microsoft\window
nt\currentversion\languagepack\surrogatefallback[plane2]
   Oueries value
                                                     HKLM\software\microsoft\window
nt\currentversion\languagepack\surrogatefallback[plane3]
                                                     HKLM\software\microsoft\windov
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
   Queries value
\label{lem:nt-current} $$ nt`currentversion\languagepack\surrogatefallback[plane7] $$ Queries value: $$ HKLM\software\microsoft\windows $$ $$
   Queries value:
\label{lem:nt-current} $$ nt`currentversion\languagepack\surrogatefallback[plane8] $$ Queries value: $$ HKLM\software\microsoft\windows $$ $$
nt\currentversion\languagepack\surrogatefallback[plane9]
Queries value: HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback[plane10]
Queries value: HKLM\software\microsoft\windows
\verb| nt\current version \language pack \surrogate fall back[plane 11]| \\
   Queries value:
                                                     HKLM\software\microsoft\windows
nt\currentversion\langu
                                                   agepack\surrogatefallback[plane12]
   Queries value
                                                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
   Oueries value
                                                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
   Oueries value
                                                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
   Oueries value
                                                     HKLM\software\microsoft\window
nt\currentversion\languagepack\surrogatefallback[plane16]
   Queries value
                                                     HKCU\control panel\desktop[smoothscroll]
    Queries value
\label{thm:local_equality} \parbox{$HKCU$\software\mbox{$\mbox{$microsoft$\windows\currentversion}$explorer\advanced[enableballoontips]} \\
   Queries value
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewalphaselect]
   Queries value
\label{like} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{tabular} list view shadow \cite{tabular} list
   Queries value
\label{localization} \mbox{HKCU} \mbox{\currentversion} \mbox{\cur
   Oueries value:
\label{thm:hkcu} \begin{tabular}{ll} HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]} \end{tabular}
                                                     HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe
   Oueries value:
ui]
   Oueries value:
                                                     HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
                                                      HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
    Queries value:
   Oueries value:
                                                     HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
   Queries value:
                                                     HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
Queries value:
HKLM \verb|\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]|
                                                     HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
   Queries value:
                                                     HKLM\hardware\devicemap\video[maxobjectnumber]
HKLM\hardware\devicemap\video[\device\video0]
    Oueries value:
    Queries value:
   Queries value
                                                     08002be10318}\0000[pruningmode]
HKLM\system\currentcontrolset\enum\display\default monitor\4&39fc21a1&0&uid0Idevicedescl
   Queries value
HKLM\system\currentcontrolset\enum\display\default monitor\4&39fc21a1&0&uid0[hardwareid]
HKLM\system\currentcontrolset\enum\display\default monitor\4&39fc21a1&0&uid0[driver]
HKLM \setminus system \setminus current control \setminus graphics drivers \setminus configuration \setminus msbdd\_noedid\_1414\_008d\_ffffffff\_ffffff_0 \setminus cc77560bc3634a486857716562968286[timestamp]
   Queries value:
Queries value
HKLM \setminus system \setminus current control set \setminus control \setminus graphics drivers \setminus configuration \setminus msbdd\_noedid\_80ee\_beef\_00000000\_00a20000\_0^ab02a9ab10912b3b7f8c017a344c8d14[setid]
HKLM \system \current control set \verb|\control| spanics drivers \verb|\connectivity| sbdd_noedid_80ee_beef_00000000_00ab02a9ab10912b3b7f8c017a344c8d14[recent] | the system \current control set \verb|\control| set \control| set \verb|\control| set \verb|\control| set \verb|\control| set \control| set \
   Queries value
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_ryi0001 agnieszka 01_1d_07d7_b2_1414_008d_ffffffff_fffffff_0^700ef59a5da31cbd79f31237af2ad4c4[timestamp]
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msh062e0 00 07db c6^182fdc0875f0a76803e4a9848a8c1ea7ftimestamol
HKLM\system\currentcontrol\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00ab02a9ab10912b3b7f8c017a344c8d14\00[primsurfsize.cx]
   Queries value:
HKLM\system\currentcontrol\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00a0000_0^ab02a9ab10912b3b7f8c017a344c8d14\00[primsurfsize.cy]
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 0^ab02a9ab10912b3b7f8c017a344c8d14\00[stride]
```

Queries value

```
HKLM\system\currentcontrol\set\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 0020000 0^ab02a9ab10912b3b7f8c017a344c8d14\00[pixelformat]
HKLM \system \current control \system \current control \system \current control \system \current \current \system \current \current \system \current \current \system \current \system \current \system \current \system \system \current \system \system \current \system \
   Oueries value
Queries value
HKLM \system \current control \system \current control \system \current \
   Queries value
Queries value
Queries value
Queries value
Oueries value
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_0020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[vsyncfreq.denominator]
   Oueries value
Oueries value
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_0020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[hsyncfreq.denominator]
   Oueries value
Hk\L^{M}\system\currentcontrolset\control\system\currentcontrolset\control\system\currentcontrol\system\currentcontrol\system\currentcontrol\system\currentcontrol\system\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\cu
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 00^ab02a9ab10912b3b7f8c017a344c8d14\00\00[scaling]
HKLM\system\currentcontrol\set\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 00ab02a9ab10912b3b7f8c017a344c8d14\00\00[rotation]
                                                        HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-
08002be10318}\0001\modes\640,480[mode1]
                                                        08002be10318}\0001\modes\640.480[mode21
                                                        HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-
08002be10318}\0001\modes\640.480[mode31
                                                        08002be10318}\0001\modes\640.480[mode4]
                                                        Queries value
08002be10318}\0001\modes\640_480[mode5]
                                                        HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-
   Queries value
08002be10318}\0001\modes\640,480[mode6]
                                                        HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-
   Queries value
08002be10318}\0001\modes\640,480[mode7]
                                                        HKLM\system\currentcontrolset\control\class\{4d36e96e-e325-11ce-bfc1-
   Queries value
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:
parameters[edid]
   Queries value:
                                                        HKLM\system\currentcontrolset\hardware
profiles\unitedvideo\control\video\{bf735b18-1b5a-4e14-b64c-
f2223c917d28}\0000[defaultsettings.bitsperpel]
\label{lem:prop} Queries \ value: $$HKLM\system\currentcontrolset\ardware profiles\united\video\control\video\ff.$$
f2223c917d28}\0000[defaultsettings.xresolution]
                                                       HKLM\system\currentcontrolset\hardware
   Queries value:
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]
                                                       HKLM\system\currentcontrolset\hardware
   Queries value:
profiles\unitedvideo\control\video\{bf735b18-1b5a-4e14-b64c
f2223c917d28}\0000[defaultsettings.flags]
                                                     HKLM\system\currentcontrolset\hardware
   Queries value:
profiles\unitedvideo\control\video\{bf735b18-1b5a-4e14-b64c-
 f2223c917d28}\0000[defaultsettings.xpanning]
\label{lem:prop} Queries \ value: \ HKLM\ system\ current control set\ hardware profiles \ united video\ control \ video\ \{bf735b18-1b5a-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b64c-4e14-b6
f2223c917d28}\0000[defaultsettings.ypanning]
Queries value: HKLM\system\currentcontrolset\hardware
```

profiles\unitedvideo\control\video\{bf735b18-1b5a-4e14-b64c-

profiles\unitedvideo\control\video\{bf735b18-1b5a-4e14-b64cf2223c917d28}\0000[defaultsettings.fixedoutput]
Queries value: HKLM\system\currentcontrolset\hardware

HKLM\system\currentcontrolset\hardware

 $\label{lem:profiles} $$ profiles \united video \control video \formalished by $$ profiles \united video \control video \formalished by $$ profiles \united video \control \formalished \control \formalished \control \formalished \control \formalished \control \con$ $profiles \verb|\united video| control \verb|\video| fbf735b18-1b5a-4e14-b64c-f2223c917d28| 0000[attach.relativey]| for the first of the first$ HKLM\svstem\currentcontrolset\hardware

 $profiles \verb|\unitedvideo| control| video| \{bf735b18-1b5a-4e14-b64c-f2223c917d28\} \\| 0000[attach.todesktop]| 10000[attach.todesktop]| 10000[attach$

f2223c917d28}\0000[defaultsettings.orientation]

Queries value:

Oueries value