Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	582
Risk Level:	4
Date Processed:	2016-04-28 13:03:06 (UTC)
Processing Time:	61.51 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\09a1d68170aa1e501c394c62bdebc8ba.exe"

Sample ID:	146
Type:	basic
Owner:	admin
Label:	09a1d68170aa1e501c394c62bdebc8ba
Date Added:	2016-04-28 12:45:05 (UTC)
File Type:	PE32:win32:gui
File Size:	672600 bytes
MD5:	09a1d68170aa1e501c394c62bdebc8ba
SHA256:	1acd2c202ca78192923a5dd2e519805e8221e0b14286925d3a1e4c3cb6add016
Description:	None

Pattern Matching Results

3 Writes to a log file [Info]
4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\windows\temp\09a1d68170aa1e501c394c62bdebc8ba.exe

["C:\windows\temp\09a1d68170aa1e501c394c62bdebc8ba.exe"]

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Creates:	C:\Users\Admin\AppData\Local\Temp\VSD4E4A.tmp
Creates:	C:\Users\Admin\AppData\Local\Temp\VSD4E4A.tmp\install.log
Opens:	C:\Windows\Prefetch\09A1D68170AA1E501C394C62BDEBC-04770F60.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\09a1d68170aa1e501c394c62bdebc8ba.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\SysWOW64\combase.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\user32.dll
Opens:	C:\Windows\SysWOW64\gdi32.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\ole32.dll
Opens:	C:\Windows\SysWOW64\shlwapi.dll
Opens:	C:\Windows\SysWOW64\shell32.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\SysWOW64\msctf.dll
Opens:	C:\Windows\SysWOW64\oleaut32.dll
Opens:	C:\Windows\SysWOW64\urlmon.dll
Opens:	C:\Windows\SysWOW64\iertutil.dll
Opens:	C:\Windows\SysWOW64\wininet.dll
Opens:	C:\Windows\SysWOW64\advapi32.dll
Opens:	C:\Windows\SysWOW64\riched20.dll
Opens:	C:\Windows\SysWOW64\usp10.dll
Opens:	C:\Windows\SysWOW64\msls31.dll
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\Windows\SysWOW64\uxtheme.dll
Opens:	C:\Users\Admin\AppData\Local\Temp\VSD4E4A.tmp
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\WindowsShell.Manifest
Opens:	C:\Windows\Fonts\micross.ttf

Opens:	C:\Windows\Fonts\tahoma.ttf
Opens:	C:\Windows\SysWOW64\dwmapi.dll
Opens:	C:\Windows\Fonts\StaticCache.dat
Opens:	C:\Windows\SysWOW64\SHCore.dll
Opens:	C:\Windows\SysWOW64\propsys.dll
Opens:	C:\
Opens:	C:\Windows\Temp
Opens:	C:\Windows\SysWOW64\cfgmgr32.dll
Opens:	C:\Windows\SysWOW64\devobj.dll
Opens:	C:\Windows\SysWOW64\setupapi.dll
Opens:	C:\Windows\Temp\FirefallInstaller.exe
Writes to:	C:\Users\Admin\AppData\Local\Temp\VSD4E4A.tmp\install.log
Reads from:	C:\Windows\Fonts\StaticCache.dat
Deletes:	C:\Users\Admin\AppData\Local\Temp\VSD4E4A.tmp

Windows Registry Events

Opens key:	HKLM\software\microsoft\wow64
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 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\system\currentcontrolset\control\session manager
Opens key:	HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key:	HKLM\system\currentcontrolset\control\nls\sorting\ids
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:	HKCU\software\microsoft\windows\currentversion\runonce
Opens key:	HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
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\09a1d68170aa1e501c394c62bdebc8ba.exe
Opens key:	HKLM\software\wow6432node\microsoft\ctf\
Opens key:	HKLM\software\wow6432node\microsoft\ctf\knownclasses
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\ms shell dlg 2

```
Opens key:              HKLM\software\wow6432node\microsoft\net framework setup\ndp\v3.5
Opens key:              HKCU\software\microsoft\windows\currentversion\explorer
Opens key:              HKLM\software\wow6432node\microsoft\windows\currentversion\explorer
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\oleaut
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\09a1d68170aa1e501c394c62bdebc8ba.exe
Opens key:              HKCU\software\classes\
Opens key:              HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder
Opens key:              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder
Opens key:              HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}\shellfolder
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-
a2d8-08002b30309d}\shellfolder
Opens key:              HKCU\software\microsoft\windows\currentversion\policies\nonenum
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\nonenum
Opens key:              HKLM\software\microsoft\windows\currentversion\policies\nonenum
Opens key:              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-
11e3-be65-806e6f6e6963}\
Opens key:              HKCU\software\classes\drive\shellex\folderextensions
Opens key:              HKCR\drive\shellex\folderextensions
Opens key:              HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-
4442-804e-409d6c4515e9}
Opens key:              HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}
Opens key:              HKLM\software\wow6432node\policies\microsoft\windows\explorer
Opens key:              HKLM\software\policies\microsoft\windows\explorer
Opens key:              HKCU\software\policies\microsoft\windows\explorer
Opens key:              HKCU\software\microsoft\windows\currentversion\explorer\
Opens key:              HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key:              HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-
97a27216f98a}\inprocserver32
Opens key:              HKCU\software\classes\directory
Opens key:              HKCR\directory
Opens key:              HKCU\software\classes\directory\shellex\iconhandler
Opens key:              HKCR\directory\shellex\iconhandler
Opens key:              HKCU\software\classes\folder
Opens key:              HKCR\folder
Opens key:              HKCU\software\classes\folder\shellex\iconhandler
Opens key:              HKCR\folder\shellex\iconhandler
Opens key:              HKCU\software\classes\allfilesystemobjects
Opens key:              HKCR\allfilesystemobjects
Opens key:              HKCU\software\classes\allfilesystemobjects\shellex\iconhandler
Opens key:              HKCR\allfilesystemobjects\shellex\iconhandler
Opens key:              HKCU\software\classes\directory\docobject
Opens key:              HKCR\directory\docobject
Opens key:              HKCU\software\classes\folder\docobject
Opens key:              HKCR\folder\docobject
Opens key:              HKCU\software\classes\allfilesystemobjects\docobject
Opens key:              HKCR\allfilesystemobjects\docobject
Opens key:              HKCU\software\classes\directory\browseinplace
Opens key:              HKCR\directory\browseinplace
Opens key:              HKCU\software\classes\folder\browseinplace
Opens key:              HKCR\folder\browseinplace
Opens key:              HKCU\software\classes\allfilesystemobjects\browseinplace
Opens key:              HKCR\allfilesystemobjects\browseinplace
Opens key:              HKCU\software\classes\directory\clsid
Opens key:              HKCR\directory\clsid
Opens key:              HKCU\software\classes\folder\clsid
Opens key:              HKCR\folder\clsid
Opens key:              HKCU\software\classes\allfilesystemobjects\clsid
Opens key:              HKCR\allfilesystemobjects\clsid
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\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}
Opens key:              HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
```

```
94f2-00a0c91efb8b}\properties
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-
11e3-be65-806e6f6e6963}\
   Opens key:                   HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\ms shell dlg
   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\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
   Queries value:               HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[09a1d68170aa1e501c394c62bdebc8ba]
   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\system\currentcontrolset\control\session manager[safedllsearchmode]
   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\microsoft\sqmclient\windows[ceipenable]
   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\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\wow6432node\microsoft\net framework setup\ndp\v3.5[sp]
   Queries value:               HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps]
   Queries value:
```

```
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer[maximizeapps]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[enableshellexecutehooks]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
    Queries value:            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
    Queries value:            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[callforattributes]
    Queries value:            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[restrictedattributes]
    Queries value:            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[foldervalueflags]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}]
    Queries value:            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32[]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-
11e3-be65-806e6f6e6963}[data]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-
11e3-be65-806e6f6e6963}[generation]
    Queries value:            HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
    Queries value:            HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
    Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
    Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showstatusbar]
    Queries value:            HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-
97a27216f98a}\inprocserver32[]
    Queries value:            HKCR\directory[docobject]
    Queries value:            HKCR\folder[docobject]
```

```
Queries value:              HKCR\allfilesystemobjects[docobject]
Queries value:              HKCR\directory[browseinplace]
Queries value:              HKCR\folder[browseinplace]
Queries value:              HKCR\allfilesystemobjects[browseinplace]
Queries value:              HKCR\directory[isshortcut]
Queries value:              HKCR\folder[isshortcut]
Queries value:              HKCR\allfilesystemobjects[isshortcut]
Queries value:              HKCR\directory[alwaysshowext]
Queries value:              HKCR\directory[nevershowext]
Queries value:              HKCR\folder[nevershowext]
Queries value:              HKCR\allfilesystemobjects[nevershowext]
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:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-
11e3-be65-806e6f6e6963}[data]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-
11e3-be65-806e6f6e6963}[generation]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
```