Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 146, Task ID: 585

Task ID: 585

Risk Level: 4

Date Processed: 2016-04-28 13:03:06 (UTC)

Processing Time: 61.15 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

Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0

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

File System Events

Creates: C:\Users\Admin\AppData\Local\Temp\VSD14DB.tmp

Creates: C:\Users\Admin\AppData\Local\Temp\VSD14DB.tmp\install.log
Opens: C:\Windows\Prefetch\09A1D68170AA1E501C394C62BDEBC-04770F60.pf

Opens: C:\Windows

Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\System32\wow64win.dll
Opens: C:\Windows\System32\wow64cpu.dll
Opens: C:\Windows\system32\wow64log.dll

Opens: C:\Windows\SysWOW64

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

 Opens:
 C:\Windows\SysWOW64\imm32.dll

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

 Opens:
 C:\Windows\SysWOW64\riched20.dll

Opens: C:\Windows\Globalization\SortIng\SortDefault.nls

Opens: C:\Windows\SysWOW64\rpcss.dll
Opens: C:\Windows\SysWOW64\uxtheme.dll
Opens: C:\Users\Admin\AppData\Local\Temp

 Opens:
 C:\

 Opens:
 C:\Users

 Opens:
 C:\Users\Admin

 Opens:
 C:\Users\Admin\AppData

 Opens:
 C:\Users\Admin\AppData\Local

Opens: C:\Users\Admin\AppData\Local\Temp\VSD14DB.tmp\

Opens: C:\windows\temp\09a1d68170aa1e501c394c62bdebc8ba.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

C:\Windows\WindowsShell.Manifest Opens: Opens: C:\Windows\Fonts\tahoma.ttf Opens: C:\windows\temp\dwmapi.dll Opens: C:\Windows\SysWOW64\dwmapi.dll Opens: C:\Windows\Fonts\StaticCache.dat Opens: C:\Windows\SysWOW64\ole32.dll Opens: C:\Windows\SysWOW64\kernel32.dll C:\windows\temp\FirefallInstaller.exe Opens: Opens: C:\windows\temp\PROPSYS.dll

Opens: C:\Windows\SysWOW64\propsys.dll
Opens: C:\Windows\SysWOW64\shell32.dll

C:\Windows\Temp Opens:

C:\Windows\Temp\FirefallInstaller.exe Opens: Opens: C:\Windows\SysWOW64\en-US\setupapi.dll.mui Opens: C:\Windows\SysWOW64\en-US\KernelBase.dll.mui

Writes to: C:\Users\Admin\AppData\Local\Temp\VSD14DB.tmp\install.log

Reads from: C:\Windows\Fonts\StaticCache.dat

Deletes: C:\Users\Admin\AppData\Local\Temp\VSD14DB.tmp

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options

HKLM\system\currentcontrolset\control\session manager Opens key:

Opens key: HKLM\software\microsoft\wow64

HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file Opens key:

execution options

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: $HKLM \verb|\software\policies\microsoft\windows\safer\codeidentifiers$ 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 HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration Opens kev:

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: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side$

Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions

Opens key: HKLM\

Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\diagnostics

HKLM\software\wow6432node\microsoft\windows Opens key:

nt\currentversion\gre_initialize

Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\compatibility32 HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime Opens kev:

compatibility

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows

HKLM\software\wow6432node\microsoft\ole Opens key: Opens key: HKLM\software\wow6432node\microsoft\ole\tracing Opens key: HKLM\software\microsoft\ole\tracing Opens key: HKLM\software\wow6432node\microsoft\oleaut Opens key: HKLM\system\currentcontrolset\services\crypt32

Opens key:

settings Opens kev:

HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings HKLM\software\policies\microsoft\windows\currentversion\internet Opens key:

settings

Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale HKCU\software\microsoft\windows\currentversion\runonce Opens key:

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\microsoft\windows nt\currentversion\fontlink\systemlink

HKLM\software\microsoft\windows Opens key:

nt\currentversion\languagepack\datastore_v1.0

HKLM\software\microsoft\windows Opens kev:

nt\currentversion\languagepack\surrogatefallback

Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\segoe ui Opens key:

HKLM\software\wow6432node\microsoft\ctf\compatibility\09a1d68170aa1e501c394c62bdebc8ba.exe

Opens key: $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07$

Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436} Opens key:

Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436} 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\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:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ 09a1d68170aa1e501c394c62bdebc8ba.exe$

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

 $Opens~key: \\ HKCU\software\microsoft\windows\currentversion\explorer\clsid\c$

3aea-1069-a2d8-08002b30309d}\shellfolder

Opens key:

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:

Opens key:

11e3-a68e-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:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ shell \ registered applications \ urlassociations \ directory \ open with progids \ microsoft \ windows \ node \ microsoft \ node \ n$

Opens key:

HKCU\software\microsoft\windows\shell\associations\urlassociations\directory

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

Opens key: HKCU\software\classes\directory\curver

Opens key: HKCR\directory\curver
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: ${\tt HKCU \backslash software \backslash classes \backslash folder \backslash browseinplace}$

Opens key: HKCR\folder\browseinplace

 ${\tt Opens\,key:} \qquad \qquad {\tt HKCU\setminus software \setminus classes \setminus all filesystemobjects \setminus browsein place}$

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\system\currentcontrolset\control\cmf\config

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\software\wow6432node\microsoft\rpc
   Opens key:
                                              HKLM\system\currentcontrolset\control\computername\activecomputername
   Opens key:
                                              HKLM\system\setup
   Opens key:
                                              HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
   Opens key:
                                              HKLM\software\policies\microsoft\windows nt\rpc
   Opens key:
                                              HKLM\software\policies\microsoft\sqmclient\windows
   Opens key:
                                              HKLM\software\microsoft\sqmclient\windows
   Opens kev:
HKCU \setminus software \setminus icrosoft \setminus ic
11e3-a68e-806e6f6e6963}\
                                              HKLM\software\microsoft\windows
   Opens kev:
nt\currentversion\languagepack\surrogatefallback\ms shell dlg
   Oueries value:
                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
   Oueries value:
                                              HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
                                              HKLM\system\currentcontrolset\control\nls\customlocale[empty]
   Oueries value:
   Oueries 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]
                                              HKCU\control panel\desktop[preferreduilanguages]
   Oueries value:
   Queries value:
                                              HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
   Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
   Queries value:
                                              HKLM\system\currentcontrolset\control\nls\sorting\versions[]
   Oueries value:
                                              {\tt HKLM \ } system \verb| current control \verb| session manager[safedll sear chmode] \\
   Queries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
   Oueries value:
                                              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[09a1d68170aa1e501c394c62bdebc8ba]
   Oueries value:
                                              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
   Oueries value:
                                              HKLM \setminus software \setminus microsoft \setminus ole[pageallocatoruse system heap] \\
   Queries value:
                                              \label{lem:hklm} \verb+Kklm \+ software \+ microsoft \+ ole \+ [page allocator system \+ heap is private]
                                              HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
   Oueries value:
   Queries value:
                                              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
                                              HKLM\software\policies\microsoft\windows\currentversion\internet
   Oueries value:
settings[security_hklm_only]
                                              HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
   Oueries value:
   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]
   Oueries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
                                              HKLM\software\microsoft\windows
   Queries value:
\verb|nt\currentversion\languagepack\datastore\_v1.0[datafilepath]|
   Queries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
   Oueries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
   Oueries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
                                              HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane4]
   Queries value:
                                              HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane5]|
                                              HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback[plane6]
   Queries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
   Oueries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
   Oueries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
                                              HKLM\software\microsoft\windows
   Queries value:
\verb|nt\currentversion\language| pack\surrogatefallback[plane10]|
   Oueries value:
                                              HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback[plane11]|
                                              HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback[plane12]
   Oueries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
   Queries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
```

HKLM\software\microsoft\windows

Oueries value:

```
nt\currentversion\languagepack\surrogatefallback[plane15]
   Oueries value:
                                                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
                                                HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
   Queries value:
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
   Queries value:
                                                HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
   Queries value:
                                                HKLM\software\wow6432node\microsoft\net framework setup\ndp\v3.5[sp]
   Queries value:
                                                 HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps]
   Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer[maximizeapps]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[enableshellexecutehooks]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
   Oueries value:
                                                HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
                                                HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[callforattributes]
   Queries value:
                                                HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[restrictedattributes]
   Oueries value:
                                                HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsfordisplay]
                                                HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[hidefolderverbs]
                                                HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[usedrophandler]
   Queries value:
                                                HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsforparsing]
                                                HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
   Queries value:
                                                HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforoverlay]
   Oueries value:
                                                HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[mapnetdriveverbs]
   Oueries value:
                                                HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforinfotip]
   Queries value:
                                                HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideinwebview]
   Queries value:
                                                HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideondesktopperuser]
                                                HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
   Queries value:
                                                HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsuniversaldelegate]
   Oueries value:
                                                HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[nofilefolderjunction]
                                                HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[pintonamespacetree]
                                                HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[hasnavigationenum]
   Queries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{20d04fe0-3aea-1069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8
08002b30309d}]
   Oueries value:
11e3-a68e-806e6f6e6963}[data]
   Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{8063a3d4-8213-42444, \ and \ baseliness \ and \ and \ baseliness \ and \
11e3-a68e-806e6f6e6963}[generation]
                                                 HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
   Queries value:
409d6c4515e9}[drivemask]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
   Oueries value:
                                                HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
   Oueries value:
```

HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]

Queries value:

HKLM\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]

Oueries 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]

Oueries value:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced| [dontprettypath] \\ \end{tabular}$

Queries value:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus advanced [showinfotip]$

Oueries value:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{\mathbb{N} indows \current version \explorer \advanced [hideicons] \end{tabular}$

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]

Queries value:

Oueries value:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{lem:hkcu} separate process \cite{lem:hkcu} advanced \cite{lem:hkcu} separate \c$

Queries value:

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]

Queries value:

 $\label{thm:linear} \begin{tabular}{ll} HKCU \software \mbox{\mathbb{N} indows \current version \explorer \advanced [showtype overlay]} \end{tabular}$

Queries value: HKCR\directory[docobject]

Queries value: HKCR\folder[docobject]

Queries value: HKCR\allfilesystemobjects[docobject]

Queries value: HKCR\directory[browseinplace]
Oueries value: HKCR\folder[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\system\currentcontrolset\control\cmf\config[system]
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error

reporting\wmr[disable]

Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]

Queries value: HKLM\software\microsoft\rpc[maxrpcsize]

Queries value:

HKLM\svstem\currentcontrolset\control\computername\activecomputername[computername]

Queries value: HKLM\system\setup[oobeinprogress]

Queries value: HKLM\system\setup[systemsetupinprogress]

Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]

Oueries value:

 $\label{thm:linear_loss} HKCU \software \mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$}\mbox{$\mbox{$}\mbox{$\mbox{$}\mbox{$}\mbox{$\mbox{$}\mbox{$}\mbox{$}\mbox{$\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$\mbox{$}$

11e3-a68e-806e6f6e6963}[data]

Queries value:

11e3-a68e-806e6f6e6963}[generation]

Queries value:

 $HKLM \verb|\software\microsoft| windows \verb|\currentversion| policies \verb|\explorer[turnoffspianimations]| \\$