Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 71, Task ID: 282

Task ID: 282

Risk Level:

2016-04-28 12:55:05 (UTC) Date Processed:

Processing Time: 61.38 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\1ecdbdc36d61f183e01cbab2fdedbf7c.exe"

Sample ID: Type: basic Owner: admin

Label: 1ecdbdc36d61f183e01cbab2fdedbf7c

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

File Type: PE32:win32:gui File Size: 779576 bytes

1ecdbdc36d61f183e01cbab2fdedbf7c MD5:

SHA256:

Description:

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

C:\windows\temp\1ecdbdc36d61f183e01cbab2fdedbf7c.exe Creates process:

["C:\windows\temp\1ecdbdc36d61f183e01cbab2fdedbf7c.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens:	<pre>C:\Windows\Prefetch\1ECDBDC36D61F183E01CBAB2FDEDB-34D3B4E9.pf</pre>
--------	--

Opens: C:\Windows

Opens: C:\Windows\System32\wow64.dll

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

C:\Windows\Temp\1ecdbdc36d61f183e01cbab2fdedbf7c.exe Opens:

Opens: C:\Windows\SysWOW64\ntdll.dll C:\Windows\SysWOW64\kernel32.dll Opens: C:\Windows\SysWOW64\KernelBase.dll Opens: 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.commoncontrols_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll

C:\Windows\SysWOW64\sechost.dll Opens: Opens: C:\Windows\SysWOW64\combase.dll C:\Windows\SysWOW64\gdi32.dll Opens: Opens: C:\Windows\SysWOW64\user32.dll Opens: C:\Windows\SysWOW64\msvcrt.dll

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

C:\Windows\SysWOW64\cryptbase.dll Opens: C:\Windows\SysWOW64\sspicli.dll Opens: Opens: C:\Windows\SysWOW64\rpcrt4.dll Opens: C:\Windows\SysWOW64\advapi32.dll C:\Windows\SysWOW64\shlwapi.dll Opens: C:\Windows\SysWOW64\shell32.dll Opens: C:\Windows\SysWOW64\ole32.dll Opens: Opens: C:\Windows\SysWOW64\imm32.dll C:\Windows\SysWOW64\msctf.dll Opens: Opens: C:\Windows\SysWOW64\oleaut32.dll Opens: C:\Windows\WindowsShell.Manifest C:\Windows\SysWOW64\uxtheme.dll Opens: C:\Windows\Fonts\sserife.fon Opens: Opens: C:\Windows\SysWOW64\dwmapi.dll

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

Opens: C:\Windows\Fonts\StaticCache.dat

Opens: C:\Program Files (x86)\EF Talk Scriber\EFTS.LIC

Opens: C:\windows\temp\EFTS.LIC C:\Windows\SysWOW64\SHCore.dll Opens: Opens:

C:\Windows\SysWOW64\clbcatq.dll Opens: Opens: C:\Windows\SysWOW64\cfgmgr32.dll Opens: C:\Windows\SysWOW64\devobj.dll C:\Windows\SysWOW64\setupapi.dll Opens:

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

Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-

4C77-AF34-C647E37CAOD9}.1.ver0x000000000000000e.db
Opens: C:\Users\desktop.ini
Opens: C:\Users

Opens: C:\Users\Admin

Opens: C:\Users\Admin\AppData

Opens: C:\Users\Admin\Desktop\desktop.ini
Reads from: C:\Windows\Fonts\StaticCache.dat

Reads from: C:\Windows\Temp\1ecdbdc36d61f183e01cbab2fdedbf7c.exe

Reads from: C:\Users\desktop.ini

Reads from: C:\Users\Admin\Desktop\desktop.ini

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\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:

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

 $\verb|nt\currentversion\compatibility32| \\$

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:

 ${\tt HKLM \ } system \verb|\ current control set \verb|\ policies \verb|\ microsoft \verb|\ cryptography \verb|\ configuration | \\$

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

 $Opens\ key: \\ HKCU \ software \ microsoft \ windows \ current version \ direct manipulation$

Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale

Opens key: HKLM\system\currentcontrolset\control\nls\locale

Opens key: HKLM\system\currentcontrol\nls\locale\alternate sorts
Opens key: HKLM\system\currentcontrol\set\control\nls\language groups
Opens key: HKLM\system\currentcontrol\set\control\session manager
Opens key: HKLM\system\currentcontrol\set\control\nls\sorting\ids

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

nt\currentversion\fontsubstitutes

Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink

Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\datastore_v1.0

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

Opens key: HKLM\software\microsoft\windows

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

nt\currentversion\languagepack\surrogatefallback\ms sans serif

Opens key: HKCU\software\efsoftware

 $Opens\ key: \\ \hspace{2.5cm} \text{HKLM} \\ software \\ \\ wow 6432 \\ node \\ \\ microsoft \\ \\ windows \\ \\ current \\ version \\$

Opens key:

Opens key

 $HKLM \label{lem:hklm} Which is the sum of the sum of$

65f9-4cf6-a03a-e3ef65729f3d}

Opens key:

65f9-4cf6-a03a-e3ef65729f3d}\propertybag

Opens key: HKCU\software\microsoft\windows\currentversion\explorer

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ session info \ 1\ known folders$

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ known foldersettings$

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:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ 1ecdbdc 36d61f183e01cbab 2fdedbf7c. execute \ descriptions \ descriptions$

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

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:

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:

Opens key: HKLM\software\microsoft\windows\currentversion\policies\nonenum

Opens key: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-

 $08002b30309d \} \verb|\inprocserver32|$

Opens key:

 $\label{thm:hkcu} \begin{tabular}{ll} HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume \end{tabular}$

Opens key:

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: HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-

a6bb2164fbd0}\inprocserver32

Opens key: HKLM\software\microsoft\com3

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

94f2-00a0c91efb8b}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-

94f2-00a0c91efb8b}\properties

Opens key: HKLM\software\microsoft\windowsruntime\clsid

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}

Opens key: HKCR\activatableclasses\clsid

Opens key: HKCR\activatableclasses\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
Opens key: HKCU\software\classes\ww6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}

Opens key: HKCR\www6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
Opens key: HKCU\software\classes\www6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\treatas

Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprochandler32

 $Opens~key: \\ HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-3$

b8dc300d9f9d}\inprochandler

Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprochandler

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\

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: ${\tt HKCU \setminus software \setminus classes \setminus all filesystemobjects \setminus clsid}$

Opens key: HKCR\allfilesystemobjects\clsid

Opens key:

 $\label{lem:hkculsoftware} HKCU software \\ \mbox{microsoft} \mbox{windows} \mbox{current} \mbox{version} \mbox{explorer} \mbox{mountpoints2} \mbox{cpc} \mbox{volume} \mbox{d5291c63-7c88-11e3-be65-806e6f6e6963} \mbox{\colorer} \mbox{explorer} \mbox{explo$

Opens key:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \$

Opens key:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma\folderdescriptions\gamma\folderdescriptions\gamma\gamma\folderdescriptions\gamma\gamm$

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}$

Opens key

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} \ property bag$

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ ctf \ compatibility \ 1ecdbdc 36d61f183e01cbab 2fdedbf7c. execond \ description \ description$

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

Opens key: HKLM\software\wow6432node\microsoft\ctf\knownclasses

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]

Queries value:

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:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [prefer external manifest] \ described by the side of the sid$

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\image file execution

options\dllnxoptions[usefilter]

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\dllnxoptions[1ecdbdc36d61f183e01cbab2fdedbf7c.exe]

```
nt\currentversion\gre_initialize[disablemetafiles]
                                     HKLM\software\wow6432node\microsoft\windows
  Queries value:
nt\currentversion\compatibility32[1ecdbdc36d61f183e01cbab2fdedbf7c]
  Queries value:
                                     HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
                                     HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Oueries value:
                                     HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  Queries value:
  Oueries value:
                                     HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:
                                     HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:
                                      HKLM\software\microsoft\ole[aggressivemtatesting]
  Oueries value:
                                     HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:
                                      HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Oueries value:
                                      HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
                                     HKLM \verb|\system| current control \verb|\system| control contr
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\language groups[1]
  Oueries value:
  Queries value:
                                      HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:
                                      HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
  Oueries value:
                                     HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
  Queries value:
                                      HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
  Oueries 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]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[acclistviewv6]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
  Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe
ui1
  Queries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
  Oueries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
  Oueries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
  Oueries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
                                     HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane3]
  Oueries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
                                     HKLM\software\microsoft\windows
  Queries value:
\verb|nt\currentversion\language| pack\surrogatefallback[plane5]|
  Queries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
  Oueries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
  Oueries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
                                     HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane9]
  Queries value:
                                     HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane10]|
                                     HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane11]
  Oueries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
  Oueries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
                                     HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane14]
  Queries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
                                     {\tt HKLM \backslash software \backslash microsoft \backslash windows}
nt\currentversion\languagepack\surrogatefallback[plane16]
                                     HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
  Queries value:
sans serifl
  Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]
  Oueries value:
65f9-4cf6-a03a-e3ef65729f3d}[category]
  Oueries value:
65f9-4cf6-a03a-e3ef65729f3d}[name]
```

HKLM\software\microsoft\windows

Oueries value:

65f9-4cf6-a03a-e3ef65729f3d}[parentfolder] Oueries value: 65f9-4cf6-a03a-e3ef65729f3d}[description] Queries value: 65f9-4cf6-a03a-e3ef65729f3d}[relativepath] Queries value: 65f9-4cf6-a03a-e3ef65729f3d}[parsingname] Oueries value: 65f9-4cf6-a03a-e3ef65729f3d}[infotip] Oueries value: 65f9-4cf6-a03a-e3ef65729f3d}[localizedname] 65f9-4cf6-a03a-e3ef65729f3d}[icon] $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ (3eb685db-10eb) \ descriptions \ descr$ 65f9-4cf6-a03a-e3ef65729f3d}[security] Queries value: 65f9-4cf6-a03a-e3ef65729f3d}[streamresource] Oueries value: 65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype] Queries value: 65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly] 65f9-4cf6-a03a-e3ef65729f3d}[roamable] Oueries value: 65f9-4cf6-a03a-e3ef65729f3d}[precreate] Oueries value: 65f9-4cf6-a03a-e3ef65729f3d}[stream] Queries value: 65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath] Oueries value: $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685db-16422 \\ node \setminus \{3eb68$ 65f9-4cf6-a03a-e3ef65729f3d}[attributes] Queries value: 65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid] Oueries value: 65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[appdata] Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel] Queries value: $HKLM \ software \ microsoft \ windows \ current version \ policies \ explorer [no set folders]$ 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-Oueries value: 08002b30309d}\shellfolder[callforattributes] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Queries value: 08002b30309d}\shellfolder[restrictedattributes] Oueries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[foldervalueflags]

08002b30309d}1 HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Queries value: 08002b30309d}\inprocserver32[] Queries value:

```
11e3-be65-806e6f6e6963}[data]
 Oueries value:
11e3-be65-806e6f6e6963}[generation]
 Queries value:
                         HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
                         HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-
 Oueries value:
a6bb2164fbd0}\inprocserver32[]
                         HKLM\software\microsoft\com3[com+enabled]
 Oueries value:
 Queries value:
                         HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
 Oueries value:
                         HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
                         HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
 Queries value:
                         HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
 Oueries value:
 Queries value:
                         HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[inprocserver32]
 Oueries value:
                         HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[]
                         HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
 Oueries value:
b8dc300d9f9d}\inprocserver32[threadingmodel]
                        HKLM\software\microsoft\ole[maxsxshashcount]
 Oueries value:
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
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]
                         HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
 Oueries value:
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
 Oueries value:
Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
 Queries value:
\label{thm:linear} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \explorer \advanced [shows tatus bar]} \end{tabular}
                         HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-
 Queries value:
97a27216f98a}\inprocserver32[]
 Queries value:
                         HKCR\directory[docobject]
 Queries value:
                         HKCR\folder[docobject]
                         HKCR\allfilesystemobjects[docobject]
 Oueries value:
                         HKCR\directory[browseinplace]
 Oueries value:
                         HKCR\folder[browseinplace]
 Oueries value:
 Queries value:
                         HKCR\allfilesystemobjects[browseinplace]
 Queries value:
                         HKCR\directory[isshortcut]
 Oueries value:
                         HKCR\folder[isshortcut]
 Oueries value:
                         HKCR\allfilesystemobjects[isshortcut]
                         HKCR\directory[alwaysshowext]
 Oueries value:
 Queries value:
                         HKCR\directory[nevershowext]
 Oueries value:
                         HKCR\folder[nevershowext]
 Oueries value:
                         HKCR\allfilesystemobjects[nevershowext]
 Oueries value:
```

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c63-7c88-4c64, d5291c63-7c88-4c64, d5291c64, d5291c64, d5291c64, d5291c64, d5291c64, d5291c64, d5291c64, d5291c644, d5291c64, d5291c64, d5291c64, d5291c64, d5291c64, d5291c64,$

11e3-be65-806e6f6e6963} [data] Queries value: $\label{lem:hcu} HKCU software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\mountpoints2| cpc \verb|\volume| {d5291c63-7c88-11e3-be65-806e6f6e6963} [generation]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$

Queries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} [name]$

Oueries value:

 $\label{lem:hklmsoftware} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder\folde$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} [description]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3adb2c-424c-b029-7fe99a87c641\} [relative path]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} \ [parsing name]$

Oueries value:

 $\label{thm:local-state} $HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}[infotip]}$

Queries value:

 $\label{localized} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma\$

Queries value

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}[stream resource]$

Oueries value:

Oueries value:

 $\label{local-continuous} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\gamma\gamm$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3adb2c-424c-b029-7fe99a87c641\} \ [roamable]$

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma\gammable b4bfcc3a-db2c-424c-b029-7fe99a87c641\}[precreate]$

Queries value:

Oueries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} [publish expanded path]$

Oueries value:

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma\fill\foldertypeid\g$

Queries value:

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[desktop]

Queries value:

 $\label{thm:local-basis} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f(1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}\category\cite{Ab3}$

Oueries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [name]$

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\f(1b3ea5dc-b587-4786-b4ef-bd1dc332aeae)\cite{lem:hklmsoftware}\cite$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [description]$

Queries value:

Oueries value:

 $\label{thm:local-continuous} HKLM \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} wow 6432 node \end{tabular} microsoft \end{tabular} windows \end{tabular} \begin{tabular}{ll} HKLM \e$

b587-4786-b4ef-bd1dc332aeae}[parsingname]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} \ [infotip]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [localized name]$

Oueries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [icon]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[security]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} \ [stream resource]$

Oueries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [stream resource type]$

Oueries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [local redirectonly]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [roamable]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[precreate]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[stream]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [publish expanded path]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[attributes]$

Oueries value:

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [initfolder \ handler]$

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}]

Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]

Queries value:

 $HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} windows \label{lem:hklm} current version \label{lem:hklm} \parbox{$>$ explorer[turnoffspianimations]$} \parbox{$$