Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 71, Task ID: 285

Task ID: 285

Risk Level: 4

Date Processed: 2016-04-28 12:55:10 (UTC)

Processing Time: 61.1 seconds
Virtual Environment: IntelliVM

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

Sample ID: 71
Type: basic
Owner: admin

Label: 1ecdbdc36d61f183e01cbab2fdedbf7c

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

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

MD5: 1ecdbdc36d61f183e01cbab2fdedbf7c

SHA256: def705b44be6093185dab301ae5f11eff75e6e077eef0a6b02cefde1c18b807f

Description: None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

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

["C:\windows\temp\1ecdbdc36d61f183e01cbab2fdedbf7c.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: \KernelObjects\MaximumCommitCondition

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

File System Events

Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches

Opens: C:\Windows\Prefetch\1ECDBDC36D61F183E01CBAB2FDEDB-34D3B4E9.pf

Opens: C:\Windows

Opens: C:\Windows\System32\wow64.dl1
Opens: C:\Windows\System32\wow64win.dl1
Opens: C:\Windows\System32\wow64cpu.dl1
Opens: C:\Windows\system32\wow64log.dl1

Opens: C:\Windows\SysWOW64

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

Opens: C:\windows\temp\1ecdbdc36d61f183e01cbab2fdedbf7c.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

Opens: C:\Windows\SysWOW64\imm32.dll
Opens: C:\Windows\WindowsShell.Manifest
Opens: C:\Windows\SysWOW64\rpcss.dll
Opens: C:\Windows\SysWOW64\uxtheme.dll
Opens: C:\Windows\Fonts\sserife.fon
Opens: C:\windows\temp\dwmapi.dll
Opens: C:\Windows\SysWOW64\dwmapi.dll

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

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

Opens: C:\Windows\Temp\1ecdbdc36d61f183e01cbab2fdedbf7c.exe
Opens: C:\Program Files (x86)\EF Talk Scriber\EFTS.LIC

Opens: C:\windows\temp\EFTS.LIC
Opens: C:\Users\Admin\AppData\Roaming
Opens: C:\Windows\SysWOW64\shell32.dll
Opens: C:\

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

 $\label{thm:cosoftwindows} Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db$

Opens: C:\windows\temp\ntmarta.dll
Opens: C:\Windows\SysWOW64\ntmarta.dll

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

4C77-AF34-C647E37CAOD9}.1.ver0x000000000000001.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

C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\Quick Opens:

Launch\User Pinned\TaskBar

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

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

Opens: C:\Windows\SysWOW64\en-US\setupapi.dll.mui

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\windows nt\currentversion\image file execution

options

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

Opens key: HKLM\software\microsoft\wow64

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

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\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

HKLM\software\policies\microsoft\mui\settings

Opens key:

Opens key:

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

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side \ microsoft \ windows \ determined \ microsoft \ microsoft \ windows \ determined \ microsoft \ mi$ Opens key:

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots

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

Opens key:

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

nt\currentversion\diagnostics HKLM\software\wow6432node\microsoft\windows Opens kev:

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\software\wow6432node\microsoft\windows nt\currentversion\windows

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

Opens key: HKLM\software\wow6432node\microsoft\ole\tracing

Opens key: HKLM\software\microsoft\ole\tracing

Opens key: $HKLM \verb|\system| current controlset \verb|\control| nls \verb|\extended| locale$

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: HKCU\software\microsoft\windows\currentversion\explorer\advanced

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

nt\currentversion\fontsubstitutes

 $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ fontsubstitutes$ Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink

HKLM\software\microsoft\windows Opens kev:

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

HKLM\software\wow6432node\microsoft\windows\currentversion Opens kev:

Opens key:

Opens key:

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\currentversion\explorer\sessioninfo\1\knownfolders

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

folders

Opens kev:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings

Opens kev:

HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer

HKLM\software\microsoft\windows\currentversion\policies\explorer Opens kev: Opens kev: HKCU\software\microsoft\windows\currentversion\policies\explorer

Opens key:

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

Opens key: HKCU\software\classes\

HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Opens key:

08002b30309d}\shellfolder

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

08002b30309d}\shellfolder

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus (20d04fe0-the following of the follow$ Opens key:

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

Opens key:

a2d8-08002b30309d}\shellfolder

HKCU\software\microsoft\windows\currentversion\policies\nonenum Opens kev:

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\policies\nonenum

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

Opens key:

11e3-a68e-806e6f6e6963}\

Opens key: HKCU\software\classes\drive\shellex\folderextensions

HKCR\drive\shellex\folderextensions Opens key:

HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-Opens key:

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: HKLM\software\microsoft\com3

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

b8dc300d9f9d}

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

b8dc300d9f9d}\treatas

 $HKCR\wow6432 node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treat as$ Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\progid

 $HKCR\wow6432 node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid$ Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\}$

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

b8dc300d9f9d}\progid

Opens key: $HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid$

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprocserver32

Opens key:

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler

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

b8dc300d9f9d}\inprochandler

Opens key: HKLM\system\currentcontrolset\control\lsa\accessproviders

Opens key: HKLM\system\currentcontrolset\services\ldap

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

Opens key:

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

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: 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:

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

Opens key:

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

Opens key:

Opens key:

 $\label{lem:hklmsoftwarewow6432} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f(1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}\propertybag$

Opens key:

Opens key: ${\tt HKLM\system\currentcontrolset\control\cmf\config}$

Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr

 $Opens~key: \\ HKLM\software\wow6432node\microsoft\windows\currentversion\setup$

 $Opens\ key: \\ \hspace{1.5cm} \text{HKLM} \\ software \\ microsoft \\ windows \\ current version \\ setup$

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

Opens key: HKLM\system\currentcontrol\set\control\computername\activecomputername

Opens key: HKLM\system\setup

Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc

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

 $Opens~key: $HKLM\software\microsoft\tip\\\{0000897b-83df-4b96-be07-0fb58b01c4a4\\\languageprofile\\0x00000000\\\{0001bea3-ed56-483d-a2e2-aeae25577436\}$

Opens key:

 $\label{thm:local-condition} HKCU software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ \{8063a3d3-8213-11e3-a68e-806e6f6e6963\} \column{tabular}{l}$

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

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

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

options[disableusermodecallbackfilter]

 $\label{lem:current} Queries \ value: \\ HKLM\ system\ current controls et\ control\ session$

manager[cwdillegalindllsearch]

Oueries value:

Queries value:

 $HKLM \verb|\system| current controlset| control \verb|\nls| language[install language fall back]|$

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:

 $\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} $$ idebyside[preferexternal manifest] $$ idebyside[preferexte$

 $\label{thm:current} Queries \ value: \\ HKLM\system\current controlset\control\nls\sorting\versions[]$

Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]

```
HKLM\software\microsoft\windows
 Oueries value:
\verb|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 \setminus software \setminus microsoft \setminus ole[pageallocatoruse system heap] \\
 Oueries value:
                       HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
 Queries value:
                       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]
 Oueries value:
                       HKLM\system\currentcontrolset\control\nls\language groups[1]
 Queries value:
                       HKCU\control panel\desktop[smoothscroll]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewalphaselect]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[acclistviewv6]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
 Queries value:
                       HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe
ui1
                       HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\datastore_v1.0[disable]
                       HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
                       HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane1]
 Queries value:
                       HKLM\software\microsoft\windows
\verb|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]
 Queries value:
                       HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
 Oueries value:
                       HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
                       HKLM\software\microsoft\windows
 Queries value:
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
nt\currentversion\languagepack\surrogatefallback[plane10]
 Oueries value:
                       HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
                       HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane12]
                       HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane13]
 Queries value:
                       HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane14]|
                       HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane15]
 Oueries value:
                       HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
                       \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ fontsubstitutes\+ [ms]
 Queries value:
sans serif]
 Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]
65f9-4cf6-a03a-e3ef65729f3d}[category]
 Oueries value:
65f9-4cf6-a03a-e3ef65729f3d}[name]
 Oueries value:
65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]
65f9-4cf6-a03a-e3ef65729f3d}[description]
 Oueries value:
65f9-4cf6-a03a-e3ef65729f3d}[relativepath]
 Oueries value:
```

```
65f9-4cf6-a03a-e3ef65729f3d}[parsingname]
    Queries 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}[infotip]
    Oueries value:
65f9-4cf6-a03a-e3ef65729f3d}[localizedname]
    Oueries value:
65f9-4cf6-a03a-e3ef65729f3d}[icon]
    Oueries value:
65f9-4cf6-a03a-e3ef65729f3d}[security]
65f9-4cf6-a03a-e3ef65729f3d}[streamresource]
    Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ folde
65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]
    Oueries value:
65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]
    Queries value:
65f9-4cf6-a03a-e3ef65729f3d}[roamable]
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[precreate]
    Queries value:
65f9-4cf6-a03a-e3ef65729f3d}[stream]
    Oueries value:
65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]
    Oueries value:
65f9-4cf6-a03a-e3ef65729f3d}[attributes]
65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]
    Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ folde
65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]
    Oueries 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]
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]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
                                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Oueries value:
08002b30309d}\shellfolder[attributes]
                                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
08002b30309d}\shellfolder[callforattributes]
                                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
08002b30309d}\shellfolder[restrictedattributes]
    Queries value:
                                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsfordisplay]
    Queries value:
                                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hidefolderverbs]
                                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Oueries value:
08002b30309d}\shellfolder[usedrophandler]
                                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
08002b30309d}\shellfolder[wantsforparsing]
    Queries value:
                                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsparsedisplayname]
                                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
08002b30309d}\shellfolder[queryforoverlay]
    Queries value:
                                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[mapnetdriveverbs]
```

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

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

Queries value:

```
08002b30309d}\shellfolder[hideinwebview]
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Oueries value:
08002b30309d}\shellfolder[hideondesktopperuser]
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
 Oueries value:
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsuniversaldelegate]
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries value:
08002b30309d}\shellfolder[nofilefolderjunction]
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries value:
08002b30309d}\shellfolder[pintonamespacetree]
 Oueries value:
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hasnavigationenum]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}1
 Queries value:
11e3-a68e-806e6f6e6963}[data]
11e3-a68e-806e6f6e6963}[generation]
                        HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
 Queries value:
409d6c4515e9}[drivemask]
 Queries value:
                        HKLM\software\microsoft\com3[com+enabled]
                        HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
 Oueries value:
 Queries value:
                        HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[inprocserver32]
 Queries value:
                        HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[]
 Oueries value:
                        b8dc300d9f9d}\inprocserver32[threadingmodel]
                        HKLM\software\microsoft\ole[maxsxshashcount]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
 Oueries value:
                        HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
 Queries value:
                        HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
 Queries value:
                        HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
 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]
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
                        HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
 Oueries value:
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
\label{lem:hccu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced| fide icons| \\ \end{tabular}
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
 Oueries value:
                        HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
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]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
 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:

 $\label{thm:local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \begin{cal} b4bfcc3a-db2c-424c-b029-7fe99a87c641 \category \end{cal} \end{cal}$

Queries value:

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

Queries value:

 $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma\folderdescriptions\gamma\folderdescriptions\gamma\gamma\gamma\folderdescriptions\gamma\gam$

Queries value:

 $\label{thm:local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folds \fold$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma[]{\colorer.pdf} \end{subarrange} Abstraction \colorer. The properties of the pr$

Queries value:

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

Queries value:

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

Oueries value:

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[localredirectonly]

Oneries value.

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

Oueries value:

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

Oueries value:

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

Queries value:

 $\label{thm:local-state} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \begin{tabular}{l} b4bfcc3a-db2c-424c-b029-7fe99a87c641} [publish expanded path] \end{tabular}$

Queries value

Queries value:

 $\label{thm:local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \current \curren$

Oueries value:

 $\label{local-software-wow6432} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}[initfolderhandler]}$

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

folders[desktop]

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(1b3ea5dc-b587-4786-b4ef-bd1dc332aeae)\cite{Category}\cite{C$

Oueries value:

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

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}[parentfolder]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[description]

Queries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[relativepath]

Oueries value

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

Oueries value:

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

Oueries value:

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

Oueries value

Queries value

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value

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

Oueries value:

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

Oueries value:

Queries value:

Oueries value

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

Queries value:

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

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\system\currentcontrol\cmf\config[system] Queries value: HKLM\software\wow6432node\microsoft\windows\windows error

reporting\wmr[disable]

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

Queries value:

Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup[systemsetupinprogress]

Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]

 $\label{lem:hkcu} HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ \{8063a3d3-8213-11e3-a68e-806e6f6e6963\} \ [data]$

Queries value:

 $\label{thm:local-prop} HKCU software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\mountpoints2| cpc \verb|\volume| {8063a3d3-8213-11e3-a68e-806e6f6e6963} [generation]$

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

Queries value:

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