Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 246, Task ID: 985

Task ID: 985

Risk Level:

Date Processed: 2016-04-28 13:14:19 (UTC)

Processing Time: 4.17 seconds Virtual Environment: IntelliVM

"c:\windows\temp\280c53057f49089a8bbef69fce3e81cd.exe" **Execution Arguments:**

Sample ID: Type: basic Owner: admin

Label: 280c53057f49089a8bbef69fce3e81cd

Date Added: 2016-04-28 12:45:15 (UTC)

File Type: PE32:win32:gui File Size: 376040 bytes

280c53057f49089a8bbef69fce3e81cd MD5:

SHA256: dcf31db18983784dcecab6c4557722cb32cc384121b5b4cc77930b071f747c25

Description:

Pattern Matching Results

Signed by adware producer [Adware, PUA]

2 PE: Nonstandard section

4 Packer: NSIS [Nullsoft Scriptable Install System]

Static Events

Anomaly: PE: Contains a virtual section

Anomaly: PE: Contains one or more non-standard sections

Process/Thread Events

C:\windows\temp\280c53057f49089a8bbef69fce3e81cd.exe Creates process:

["C:\windows\temp\280c53057f49089a8bbef69fce3e81cd.exe"]

Terminates process: C:\Windows\Temp\280c53057f49089a8bbef69fce3e81cd.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex Creates event: \KernelObjects\MaximumCommitCondition

File System Events

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

Creates: C:\Users\Admin\AppData\Local\Temp\

Creates: C:\Users\Admin\AppData\Local\Temp\nsbCE1D.tmp C:\Users\Admin\AppData\Local\Temp\nscCFA5.tmp Creates:

Creates: C:\Users C:\Users\Admin Creates:

C:\Users\Admin\AppData Creates: C:\Users\Admin\AppData\Local Creates: C:\Users\Admin\AppData\Local\Temp Creates:

Creates: $C: \verb|\USers\Admin\AppData\Local\Temp\nscCFA5.tmp\tkDecript.dll|$ Creates: C:\Users\Admin\AppData\Local\Temp\nscCFA5.tmp\version.dll Opens: C:\Windows\Prefetch\280C53057F49089A8BBEF69FCE3E8-6305A30E.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

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

Opens: C:\windows\temp\280c53057f49089a8bbef69fce3e81cd.exe.Local\

Opens: C:\Windows\winsxs\x86_microsoft.windows.common-

controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af

C:\Windows\winsxs\x86_microsoft.windows.common-Opens: controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll

C:\windows\temp\VERSION.dll Opens: C:\Windows\SysWOW64\version.dll Opens: Opens: C:\Windows\SysWOW64\apphelp.dll Opens: C:\Windows\AppPatch\sysmain.sdb

C:\Windows\Temp\280c53057f49089a8bbef69fce3e81cd.exe Opens:

Opens: C:\Windows\AppPatch\AcGenral.dll C:\windows\temp\UxTheme.dll Opens: Opens: C:\Windows\SysWOW64\uxtheme.dll C:\windows\temp\WINMM.dll Opens: Opens: C:\Windows\SysWOW64\winmm.dll Opens: C:\windows\temp\samcli.dll

```
Opens:
                         C:\Windows\SysWOW64\samcli.dll
                        C:\windows\temp\MSACM32.dll
 Opens:
 Opens:
                        C:\Windows\SysWOW64\msacm32.dll
 Opens:
                        C:\windows\temp\sfc.dll
                        C:\Windows\SysWOW64\sfc.dll
 Opens:
 Opens:
                        C:\windows\temp\sfc_os.DLL
                        C:\Windows\SysWOW64\sfc_os.dll
 Opens:
 Opens:
                        C:\windows\temp\USERENV.dll
 Opens:
                        C:\Windows\SysWOW64\userenv.dll
 Opens:
                        C:\windows\temp\profapi.dll
                        C:\Windows\SysWOW64\profapi.dll
 Opens:
 Opens:
                        C:\windows\temp\dwmapi.dll
 Opens:
                        C:\Windows\SysWOW64\dwmapi.dll
                        C:\windows\temp\MPR.dll
 Opens:
 Opens:
                        C:\Windows\SysWOW64\mpr.dll
                        C:\windows\temp\280c53057f49089a8bbef69fce3e81cd.exe.Manifest
 Opens:
 Opens:
                        C:\Windows\SysWOW64\imm32.dll
                        C:\Windows\SysWOW64\en-US\setupapi.dll.mui
 Opens:
                        C:\Windows\SysWOW64\rpcss.dll
 Opens:
 Opens:
                        C:\windows\temp\SHFOLDER.DLL
 Opens:
                        C:\Windows\SysWOW64\shfolder.dll
                        C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens:
 Opens:
                        C:\Windows\SysWOW64\shell32.dll
                        C:\Windows\winsxs\x86_microsoft.windows.common-
 Opens:
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
                         C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
                        C:\Windows\WindowsShell.Manifest
 Opens:
 Opens:
                        C:\
                        C:\Windows\SysWOW64\propsys.dll
 Opens:
 Opens:
                        Opens:
                        C:\windows\temp\ntmarta.dll
 Opens:
                        C:\Windows\SysWOW64\ntmarta.dll
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
 Opens:
4C77-AF34-C647E37CA0D9}.1.ver0x000000000000001.db
                        C:\Users\Admin\Desktop\desktop.ini
 Opens:
 Opens:
                        C:\Users\Admin\AppData\Local\Temp
 Opens:
                        C:\Users\Admin\AppData\Local\Temp\nsbCE1D.tmp
 Opens:
                        C:\Users
 Opens:
                        C:\Users\Admin
                        C:\Users\Admin\AppData
 Opens:
 Opens:
                        C:\Users\Admin\AppData\Local
                        C:\Users\Admin\AppData\Local\Temp\nscCFA5.tmp
 Opens:
 Opens:
                        C:\Users\Admin\AppData\Local\Temp\nscCFA5.tmp\tkDecript.dll
 Opens:
                        C:\Users\Admin\AppData\Local\Temp\nscCFA5.tmp\version.dll
 Writes to:
                        {\tt C:\Users\Admin\AppData\Local\Temp\nscCFA5.tmp\tkDecript.dll}
 Writes to:
                        C:\Users\Admin\AppData\Local\Temp\nscCFA5.tmp\version.dll
 Reads from:
                        C:\Users\Admin\Desktop\desktop.ini
 Reads from:
                         C:\Windows\Temp\280c53057f49089a8bbef69fce3e81cd.exe
 Deletes:
                        C:\Users\Admin\AppData\Local\Temp\nsbCE1D.tmp
 Deletes:
                        C:\Users\Admin\AppData\Local\Temp\nscCFA5.tmp
 Deletes:
                        C:\Users\Admin\AppData\Local\Temp\nscCFA5.tmp\tkDecript.dll
                        C:\Users\Admin\AppData\Local\Temp\nscCFA5.tmp\version.dll
 Deletes:
```

Windows Registry Events

Opens key:

options

- 1	
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\software\microsoft\wow64
Opens key:	<pre>HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file</pre>
execution options	
Opens key:	<pre>HKLM\system\currentcontrolset\control\safeboot\option</pre>
Opens key:	<pre>HKLM\system\currentcontrolset\control\srp\gp\dll</pre>
Opens key:	
HKLM\software\wow6432	node\policies\microsoft\windows\safer\codeidentifiers
Opens key:	<pre>HKLM\software\policies\microsoft\windows\safer\codeidentifiers</pre>
Opens key:	<pre>HKCU\software\policies\microsoft\windows\safer\codeidentifiers</pre>
Opens key:	<pre>HKLM\system\currentcontrolset\control\nls\customlocale</pre>
Opens key:	<pre>HKLM\system\currentcontrolset\control\nls\language</pre>
Opens key:	<pre>HKLM\system\currentcontrolset\control\mui\uilanguages</pre>
Opens key:	<pre>HKLM\system\currentcontrolset\control\mui\uilanguages\en-us</pre>
Opens key:	<pre>HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete</pre>
Opens key:	<pre>HKLM\software\wow6432node\policies\microsoft\mui\settings</pre>
Opens key:	<pre>HKLM\software\policies\microsoft\mui\settings</pre>
Opens key:	HKCU\
Opens key:	<pre>HKCU\control panel\desktop\muicached\machinelanguageconfiguration</pre>
Opens key:	<pre>HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration</pre>
Opens key:	<pre>HKCU\software\policies\microsoft\control panel\desktop</pre>
Opens key:	<pre>HKCU\control panel\desktop\languageconfiguration</pre>
Opens key:	HKCU\control panel\desktop
Opens key:	<pre>HKCU\control panel\desktop\muicached</pre>

HKLM\software\microsoft\windows nt\currentversion\image file execution

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

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags

Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\windows file

protection

Opens key: HKLM\software\policies\microsoft\windows nt\windows file protection

Opens key: HKLM\

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

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

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\software\wow6432node\microsoft\oleaut

Opens key: HKLM\system\currentcontrolset\control\cmf\config Opens key: $\label{thm:local_microsoft} \begin{tabular}{ll} HKLM\software\wow6432node\microsoft\windows\windows\end{tabular} error\ reporting\wmr$

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

Opens key: HKLM\software\microsoft\windows\currentversion\setup Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale

Opens key: HKLM\system\currentcontrolset\services\crypt32

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

settings Opens key:

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

settings

Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder

Opens key:

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 \ 280c53057f49089a8bbef69fce3e81cd. exemple \ applications \$

HKCU\software\classes\ Opens key:

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:

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

Opens key:

a2d8-08002b30309d}\shellfolder

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

Opens key:

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

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

Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume

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}

HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-Opens key:

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\

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

Opens kev:

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

Opens key:

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

Opens key: HKCU\software\classes\directory

HKCR\directory Opens key:

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

Opens key: HKCR\directory\curver

```
Opens key: HKCR\directory\
Opens key: HKCU\software\c
```

s 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:

Opens key:

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

Opens key:

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

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

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ \ explorer \ \ session in folders$

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

folders

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

Opens key: $\begin{tabular}{ll} HKCR \ww6432 node \clsid {1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} \treat as Opens key: \\ b8dc300d9f9d} \progid \\ HKCU \software \classes \ww6432 node \clsid {1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} \end{tabular}$

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

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-

b8dc300d9f9d}\inprochandler

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

b8dc300d9f9d}\inprochandler

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

 $Opens\ key: \\ HKLM\system\currentcontrolset\control\computername\active computername$

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

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

Opens key:

 $HKLM \setminus software \setminus wow 6432 node \\ \mbox{microsoft} \setminus windows \setminus current \\ \mbox{version} \setminus explorer \setminus known folders \\ \mbox{ettings}$

Opens key:

```
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-16der \ and \ baselines \ explorer \ e
b587-4786-b4ef-bd1dc332aeae}
       Opens key:
HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{1b3ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4ea5dc-1b4e
b587-4786-b4ef-bd1dc332aeae}\propertybag
65f9-4cf6-a03a-e3ef65729f3d}
       Opens key:
65f9-4cf6-a03a-e3ef65729f3d}\propertybag
       Opens kev:
HKLM \label{lem:hklm} Which is the second of the second 
0e22-4760-9afe-ea3317b67173}
       Opens key:
0e22-4760-9afe-ea3317b67173}\propertybag
                                                                                                            HKLM\software\wow6432node\microsoft\windows
       Opens key:
nt \verb|\currentversion| profile list \verb|\s-1-5-21-980053277-1733835069-2361817685-1001| list list \verb|\s-1-5-21-980053277-1733885-1001| list \verb|\s-1-5-21-98005327-1001| list \verb|\s-1-5-21-9800
                                                                                                           HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
       Opens kev:
 980053277-1733835069-2361817685-1001
       Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-
 11e3-a68e-806e6f6e6963}\
       Opens key:
                                                                                                            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
       Opens key:
                                                                                                           HKLM\software\wow6432node\microsoft\rpc\extensions
       Opens key:
                                                                                                           HKLM\software\microsoft\rpc\extensions
       Queries value:
                                                                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
       Queries value:
                                                                                                           HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
       Oueries 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]
                                                                                                           HKLM\system\currentcontrolset\control\mui\uilanguages\en-
       Queries value:
us[alternatecodepage]
       Queries value:
                                                                                                           HKCU\control panel\desktop[preferreduilanguages]
       Queries value:
                                                                                                            HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
       Oueries value:
HKCU\software\microsoft\windows
       Oueries value:
```

nt\currentversion\appcompatflags[showdebuginfo]

HKLM\system\currentcontrolset\control\nls\sorting\versions[] Queries value: Queries value: HKLM\software\policies\microsoft\windows nt\windows file

protection[knowndlllist]

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

HKLM\software\microsoft\windows Queries value: nt\currentversion\gre_initialize[disablemetafiles]

Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[280c53057f49089a8bbef69fce3e81cd] Oueries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\windows[loadappinit_dlls]

HKLM\software\microsoft\ole[pageallocatorusesystemheap] Oueries value: Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Queries value: HKLM\system\currentcontrolset\control\cmf\config[system] Queries value: HKLM\software\wow6432node\microsoft\windows\windows error

reporting\wmr[disable]

HKLM\software\microsoft\windows\currentversion\setup[sourcepath] Queries value: Queries value: $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| currentversion[device path]|$

Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[en-us] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us] Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings[disableimprovedzonecheck]

HKLM\software\policies\microsoft\windows\currentversion\internet Oueries value:

settings[security_hklm_only]

Queries value:

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

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ policies \ \ explorer \ [no properties recyclebin]$

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

Oueries 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]
 Queries value:
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[restrictedattributes]
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries value:
08002b30309d}\shellfolder[wantsfordisplay]
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries value:
08002b30309d}\shellfolder[hidefolderverbs]
 Oueries value:
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[usedrophandler]
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Oueries value:
08002b30309d}\shellfolder[wantsforparsing]
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Oueries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
 Queries value:
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforoverlay]
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Oueries value:
08002b30309d}\shellfolder[mapnetdriveverbs]
 Queries value:
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforinfotip]
 Queries value:
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideinwebview]
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Oueries value:
08002b30309d}\shellfolder[hideondesktopperuser]
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Oueries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries value:
08002b30309d}\shellfolder[wantsuniversaldelegate]
 Queries value:
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
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]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}1
 Queries value:
11e3-a68e-806e6f6e6963}[data]
 Oueries value:
11e3-a68e-806e6f6e6963}[generation]
                        HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
 Queries value:
409d6c4515e9}[drivemask]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
 Queries value:
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
 Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ explorer \ [classicshell]
 Queries value:
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]
 Queries value:
                        HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
 Queries value:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \current version \explorer \advanced [hideicons] \end{tabular}
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
 Oueries value:
                        HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
```

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value: 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]

 $\label{lem:continuous} Queries \ value: \\ HKCR \ all filesystemobjects [nevershowext]$

Queries value:

Oueries value:

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

Queries value:

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\begin{tabular}{l} b4bfcc3a-db2c-424c-b029-7fe99a87c641\end{tabular} \end{tabular} Is ecurity \end{tabular}$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value

 $\label{linear_ham} HKLM software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder descriptions \folder \fo$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

folders[desktop]

Queries value: HKLM\software\microsoft\com3[com+enabled]

Oueries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]

Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprocserver32[threadingmodel]

Queries value: HKLM\software\microsoft\ole[maxsxshashcount]
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\system\currentcontrolset\control\lsa\accessproviders[martaextension]

Queries 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:

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

Oueries value:

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

Queries value:

Oueries value:

Oueries value:

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

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fill 1b3ea5dc-b587-4786-b4ef-bd1dc332 aeae \cite{linfotip} \end{substitute}$

Oueries value

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

Queries value:

 $\label{limit} $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions \currentversion\explorer\folder descriptions \currentversion\explorer\folder descriptions \currentversion\explorer\folder descriptions \currentversion\explorer\folder descriptions \currentversion\explorer\folder$

Queries value:

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

Queries value:

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

Oueries value

Queries value:

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

Queries value:

Queries value:

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

Oueries value:

 $\label{thm:hammon} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \fill 1b3ea5dc-b587-4786-b4ef-bd1dc332aeae \fill [stream]$

Queries value:

Queries value:

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

Queries value:

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

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}[initfolderhandler]

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

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

Queries value:

Queries value:

 $HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d} \label{fig:higher} \end{substitute}$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [parent folder]$

Ougries value

Oueries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[parsing name]$

Queries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [localized name]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [icon]$

Queries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [stream resource]$

Queries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [local redirectonly]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [roamable]$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder 6569-4cf6-a03a-e3ef65729f3d \cite{lem:hklmsoftware} \end{substitute} folder \cite{lem:hklmsoftware} \end{substitute} The label \cite{lem:hklmsoftware} \end{substitute} The label \cite{lem:hklmsoftware} \cite{l$

Queries value:

 $\label{limits} $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\[stream]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [publish expanded path]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[attributes]$

Queries value:

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

Queries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [initfolder \ handler]$

Queries value:

 $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ user shell$

folders[appdata]

Queries value:

 $\label{thm:local-ham} $$HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[category]$$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [name]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [parent folder]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [description]$

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [parsing name]$

Queries value:

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

Oueries value:

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

Oueries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1}{2} \current \folder \footnote{1}{2} \current \footnote{1} \current \footnote{1}{2} \$

Oueries value:

 $\label{thm:local-ham} $$HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[security]$$

Queries value:

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [stream resource type]$

Oueries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f$

Queries value:

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

Queries value

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [stream]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [publish \ expanded \ path]$

Oueries value:

 $\label{limit} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[attributes]}$

Oueries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [initfolder \ handler]$

Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001[profileimagepath]

Queries value:

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

Queries value:

 $\label{thm:local-condition} HKCU software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ \{8063a3d3-8213-11e3-a68e-806e6f6e6963\} \cite{Microsoft} \mbox{ [generation]} \label{thm:local-condition}$

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[version.dll]

Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll]