Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 218, Task ID: 870

Task ID: 870

Risk Level: 4

Date Processed: 2016-04-28 13:11:38 (UTC)

Processing Time: 2.21 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\afdd75bce006a193064e6227738b4bea.exe"

Sample ID: 218
Type: basic
Owner: admin

Label: afdd75bce006a193064e6227738b4bea

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

File Type: PE32:win32:gui File Size: 176199 bytes

MD5: afdd75bce006a193064e6227738b4bea

SHA256: 03f36b2c7ea1856849d6a32ee216580778c34f95d50cdf6a1a9af3f37087aaf9

Description: None

Pattern Matching Results

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

Creates process: C:\windows\temp\afdd75bce006a193064e6227738b4bea.exe

["C:\windows\temp\afdd75bce006a193064e6227738b4bea.exe"]

Terminates process: C:\Windows\Temp\afdd75bce006a193064e6227738b4bea.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

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

Creates: C:\Users\Admin\AppData\Local\Temp\nsaB26.tmp

Opens: C:\Windows\Prefetch\AFDD75BCE006A193064E6227738B4-26AA02F1.pf

Opens: C:\Windows

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

Opens: C:\Windows\SysWOW64

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

Opens: C:\Windows\Temp\afdd75bce006a193064e6227738b4bea.exe

Opens: C:\Windows\SysWOW64\ntdll.dll
Opens: C:\Windows\SysWOW64\kernel32.dll
Opens: C:\Windows\SysWOW64\KernelBase.dll
Opens: C:\Windows\apppatch\sysmain.sdb

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

controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954

 $Opens: C: \windows \winsx $x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954 \comctl32.dll$

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

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

Opens: C:\Windows\SysWOW64\cryptbase.dll C:\Windows\SysWOW64\sspicli.dll Opens: C:\Windows\SysWOW64\rpcrt4.dll Opens: C:\Windows\SysWOW64\shlwapi.dll Opens: C:\Windows\SysWOW64\shell32.dll Opens: Opens: C:\Windows\SysWOW64\advapi32.dll Opens: C:\Windows\SysWOW64\ole32.dll Opens: C:\Windows\SysWOW64\imm32.dll C:\Windows\SysWOW64\msctf.dll Opens: C:\Windows\SysWOW64\oleaut32.dll Opens: Opens: C:\Windows\SysWOW64\uxtheme.dll C:\Windows\SysWOW64\shfolder.dll Opens: Opens: C:\Windows\SysWOW64\SHCore.dll

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

Opens: C:\

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

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

 4C77-AF34-C647E37CA0D9}.1.ver0x00000000000000e.db

 Opens:
 C:\Windows\SysW0W64\desktop.ini

 Opens:
 C:\Users\Admin\Desktop\desktop.ini

 Opens:
 C:\Windows\SysW0W64\cfgmgr32.dl1

 Opens:
 C:\Windows\SysW0W64\devobj.dl1

Opens: C:\Windows\SysWOW64\cfgmgr32.dl1
Opens: C:\Windows\SysWOW64\devobj.dl1
Opens: C:\Windows\SysWOW64\setupapi.dl1
Opens: C:\Windows\SysWOW64\profapi.dl1

Opens: C:\Users\Admin\AppData\Local\Temp\nsaB26.tmp

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

Reads from: C:\Windows\Temp\afdd75bce006a193064e6227738b4bea.exe

Deletes: C:\Users\Admin\AppData\Local\Temp\nsaB26.tmp

Windows Registry Events

Opens key: HKLM\software\microsoft\wow64

Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key:

HKLM\softwa Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers

Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers

Opens key: HKLM\system\currentcontrol\set\control\nls\customlocale

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

HKLM\system\currentcontrolset\control\mi\uilanguages

Opens key: HKLM\system\currentcontrolset\control\nis\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

HKLM\software\policies\microsoft\windows\safer\codeidentifiers

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\system\currentcontrolset\control\session manager

 $Opens \ key: \\ HKLM\ software\ wow 6432 node\ microsoft\ windows \\ nt\ current version\ gre_initialize$

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32

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

compatibility

Opens key: HKLM

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

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

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

Opens key:

 $\label{thm:linear} \begin{tabular}{ll} HKLM \end{tabular} is system \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} is system \end{tabular} \begin{tabular}{ll} configuration \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} \begin{tabular}{ll} configuration \e$

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: ${\tt HKLM \setminus software \setminus microsoft \setminus sqmclient \setminus windows}$

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

Opens key:

Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ afdd 75 bce 006 a 1930 64 e 6227738 b4 bea. exemple the shell compatibility \ applications \ afdd 75 bce 006 a 1930 64 e 6227738 b4 bea. exemple the shell compatibility \ applications \ afdd 75 bce 006 a 1930 64 e 6227738 b4 bea. exemple the shell compatibility \ applications \ afdd 75 bce 006 a 1930 64 e 6227738 b4 bea. exemple the shell compatibility \ applications \ afdd 75 bce 006 a 1930 64 e 6227738 b4 bea. exemple the shell compatibility \ applications \ afdd 75 bce 006 a 1930 64 e 6227738 b4 bea. exemple the shell compatibility \ applications \ afdd 75 bce 006 a 1930 64 e 6227738 b4 bea. exemple the shell compatibility \ applications \ afdd 75 bce 006 a 1930 64 e 6227738 b4 bea. exemple the shell compatibility \ applications \ afdd 75 bce 006 a 1930 64 e 6227738 b4 bea. exemple the shell compatibility \ applications \ afdd 75 bce 006 a 1930 64 e 6227738 b4 bea. exemple the shell compatibility \ applications \ afdd 75 bce 006 a 1930 64 e 6227738 b4 bea. exemple the shell compatibility \ applications \ afdd 75 bce 006 a 1930 64 e 6227738 b4 bea. exemple the shell compatibility \ applications \ afdd 75 bce 006 a 1930 64 e 6227738 b4 bea. exemple the shell compatibility \ applications \ afdd 75 bce 006 a 1930 64 e 6227738 b4 bea. exemple the shell compatibility \ applications \ afdd 75 bce 006 a 1930 64 e 6227738 b4 bea. exemple the shell compatibility \ applications \ afdd 75 bce 006 a 1930 64 e 6227738 b4 bea. exemple the shell compatibility \ applications \ afdd 75 bce 006 a 1930 64 e 6227738 b4 bea. exemple the shell compatibility \ applications \ afdd 75 bce 006 a 1930 64 e 6227738 b4 bea. exemple the shell compatibility \ applications \ afdd 75 bce 006 a 1930 64 e 6227738 b4 bea. exemple the shell compatibility \ applications \ afdd 75 bce 006 a 1930 64 e 6227738 b4 bea. exemple the shell compatibility \ applications \ afdd 75 bce 006 a 1930 64 e 6227738 b4 bea. exemple the shell compatibili$

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\{20d04fe0-

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

Opens key:

a2d8-08002b30309d}\shellfolder

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

Opens key:

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

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

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

08002b30309d}\inprocserver32

Opens key:

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

Opens kev:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mountpoints 2 \setminus cpc \setminus volume \setminus \{d5291c64-7c88-d124, d244, d24$

11e3-be65-806e6f6e6963}\

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

Opens key: HKCR\drive\shellex\folderextensions

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

Opens key: HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-

97a27216f98a}\inprocserver32

HKCU\software\classes\directory Opens key:

Opens key: HKCR\directory

Opens key: HKCU\software\classes\directory\shellex\iconhandler

Opens key: HKCR\directory\shellex\iconhandler Opens key: HKCU\software\classes\folder

HKCR\folder Opens key:

Opens key: HKCU\software\classes\folder\shellex\iconhandler

HKCR\folder\shellex\iconhandler Opens key: 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: HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-

a6bb2164fbd0}\inprocserver32

Opens key: HKLM\software\microsoft\com3

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

Opens key:

b8dc300d9f9d}

Opens key: HKCR\activatableclasses\clsid

Opens key: HKCR\activatableclasses\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}

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

b8dc300d9f9d}\treatas

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprocserver32

 $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{1f486a52 - 3cb1 - 48fd - 8f50 - 8f50 - 48fd - 8f50 - 8f50$ Opens key:

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\inprochandler

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

b8dc300d9f9d}\inprochandler

Opens key:

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

Opens kev:

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

Opens key:

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

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

Opens key:

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

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

folders Opens key:

Opens kev:

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

Opens key:

Opens key:

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

Opens key:

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

Opens key:

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

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

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

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

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

94f2-00a0c91efb8b}

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

94f2-00a0c91efb8b}\properties

Opens key:

 $\label{thm:local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder folder descriptions\folder folder descriptions\folder folder folder descriptions\folder folder fo$

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

nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001

1923240461-1905901954-2556564120-1001

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

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

Queries value:

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

Queries value:

HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]

Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]

Oueries 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:

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

Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]

Queries value: HKCU\software\microsoft\windows

nt\currentversion\appcompatflags[showdebuginfo]

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

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

Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[afdd75bce006a193064e6227738b4bea]
Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\windows[loadappinit_dlls]

Queries value: HKLM\system\currentcontrol\sa\fipsalgorithmpolicy[enabled]

Queries value: HKLM\system\currentcontrol\sa[fipsalgorithmpolicy]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]

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

Queries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer[no properties my computer]$

Queries value:

```
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
   Queries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ explorer [no set folders]
   Oueries value:
\label{thm:local_hammon} \begin{tabular}{l} HKLM \software \verb|\microsoft| windows \current version \policies \explorer[nointerneticon] \end{tabular}
                                                   HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
   Oueries value:
                                                   HKLM\svstem\currentcontrolset\control\nls\extendedlocale[en-us]
   Queries value:
                                                   HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
   Queries value:
                                                   HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
   Oueries value:
                                                   HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
   Queries value:
                                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
   Queries value:
                                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[callforattributes]
                                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[restrictedattributes]
                                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[foldervalueflags]
   Queries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{20d04fe0-3aea-1069-a2d8-44e1-44e1\}] \ descriptions \ description \ for the software \ description \ descrip \ description \ description \ description \ description \ descr
08002b30309d}]
                                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\inprocserver32[]
   Oueries value:
11e3-be65-806e6f6e6963}[data]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-
11e3-be65-806e6f6e6963}[generation]
   Queries value:
                                                   HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
   Oueries value:
                                                   HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
   Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ explorer [nonet crawling]
                                                   HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
   Queries 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:
\label{lem:hkcu} \verb+kkcu\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]+ of the lemma of the le
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
                                                   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]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
   Queries value:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced[iconsonly]| \\ \end{tabular}
   Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced [show type overlay]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showstatusbar]
   Queries value:
                                                   HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-
97a27216f98a}\inprocserver32[]
                                                   HKCR\directory[docobject]
   Queries value:
   Queries value:
                                                   HKCR\folder[docobject]
   Queries value:
                                                   HKCR\allfilesystemobjects[docobject]
```

Queries value: HKCR\directory[browseinplace]
Oueries 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: HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-

a6bb2164fbd0}\inprocserver32[]

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

Queries 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\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-

db2c-424c-b029-7fe99a87c641}[category]

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

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:

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

Queries value:

 $\label{local-ham} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma\$

Queries value

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

Queries value:

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

Queries value:

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

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:

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

Queries value:

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

folders[desktop]

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:

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

Oueries value:

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

Queries value:

 $\label{thm:microsoftwindows} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\f(1b3ea5dc-b587-4786-b4ef-bd1dc332 aeae\}\[relative path]$

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

Oueries value:

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

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:

Oueries value

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

Oueries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\\folderdescriptions\\\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[attributes]$

Oueries value:

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

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:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value

65f9-4cf6-a03a-e3ef65729f3d}[parsingname]

Queries value:

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

Queries value:

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

Oueries value

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

Oueries value:

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

Oueries value:

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

Oueries value

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

Queries value

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value

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

Queries value:

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

Queries value:

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

Queries value:

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

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

folders[appdata]

Queries value:

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

Queries value:

 $\label{limits} $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[name]}$

Queries value:

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

Queries value: HKLM\software\wow6432node\microsoft\windows\windows error

reporting\wmr[disable]

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

Queries value:

Queries value:

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

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsingname]

Oueries value

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{array} In construction \end{array} The substruction \en$

Queries value:

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

Queries value:

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

Oueries value:

0e22-4760-9afe-ea3317b67173}[streamresource]

Oueries value:

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

Queries value:

 $\label{thm:local-condition} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdes$

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value

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

Queries value:

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

Oueries 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-1-5-21-1923240461-1905901954-2556564120-1001[profileimagepath]

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