# Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 251, Task ID: 1002

Task ID: 1002

Risk Level:

2016-04-28 13:14:59 (UTC) Date Processed:

Processing Time: 61.14 seconds Virtual Environment: IntelliVM

"c:\windows\temp\b9157cdd8f2376b26202cce9b65f1efb.exe" **Execution Arguments:** 

Sample ID: Type: basic Owner: admin

Label: b9157cdd8f2376b26202cce9b65f1efb

Date Added: 2016-04-28 12:45:16 (UTC)

File Type: PE32:win32:gui File Size: 450907 bytes

b9157cdd8f2376b26202cce9b65f1efb MD5:

SHA256: 38a24c7531054711addae1e035f29a9c5e4772890c023481427945c19e2ef417

Description:

# 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

C:\windows\temp\b9157cdd8f2376b26202cce9b65f1efb.exe

["C:\windows\temp\b9157cdd8f2376b26202cce9b65f1efb.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\nsu848.tmp

C:\Windows\Prefetch\B9157CDD8F2376B26202CCE9B65F1-19879722.pf Opens:

Opens: C:\Windows

Opens: C:\Windows\System32\wow64.dll Opens: C:\Windows\SysWOW64

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

C:\Windows\Temp\b9157cdd8f2376b26202cce9b65f1efb.exe Opens:

C:\Windows\SysWOW64\ntdll.dll Opens: C:\Windows\SysWOW64\kernel32.dll Opens: 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\WinSxS\x86\_microsoft.windows.commoncontrols\_6595b64144ccf1df\_5.82.9200.16384\_none\_bf100cd445f4d954\comctl32.dll

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

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

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

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

C:\Windows\SysWOW64\SHCore.dll

Opens: C:\

Opens:

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

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

4C77-AF34-C647E37CA0D9}.1.ver0x00000000000000e.db Opens: C:\Windows\SysWOW64\desktop.ini C:\Users\Admin\Desktop\desktop.ini Opens: Opens: C:\Windows\SysWOW64\profapi.dll Opens: C:\Windows\SysWOW64\cfgmgr32.dll C:\Windows\SysWOW64\devobj.dll Opens:

C:\Windows\SysWOW64\setupapi.dll Opens: C:\Users\Admin\AppData\Local\Temp\nsu848.tmp

C:\Windows\SysWOW64\riched20.dll Opens: Opens: C:\Windows\SysWOW64\usp10.dll C:\Windows\SysWOW64\msls31.dll Opens: Opens: C:\Windows\Fonts\tahoma.ttf Opens: C:\Windows\SysWOW64\dwmapi.dll

Opens: C:\Windows\win.ini

Opens:

Opens: C:\Windows\SysWOW64\uxtheme.dll.Config

C:\Windows\WinSxS\x86\_microsoft.windows.common-Opens:

controls\_6595b64144ccf1df\_6.0.9200.16384\_none\_893961408605e985

C:\Windows\WinSxS\x86\_microsoft.windows.common-Opens: controls\_6595b64144ccf1df\_6.0.9200.16384\_none\_893961408605e985\comctl32.dll

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

Reads from: C:\Windows\Temp\b9157cdd8f2376b26202cce9b65f1efb.exe

Reads from: C:\Windows\win.ini

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

Deletes: C:\Users\Admin\AppData\Local\Temp\nsu848.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:

Opens kev: 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  ${\tt HKLM \ } system \verb|\ current control \verb|\ mui \ uilanguages \verb|\ pending delete| \\$ Opens key:

Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings

Opens kev: 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

HKCU\software\policies\microsoft\control panel\desktop Opens key: Opens key: HKCU\control panel\desktop\languageconfiguration

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

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

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:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side \ as sembly storage roots$ 

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

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:local_hammon} software \wow 6432 node \end{tabular} node \end{tabular} in the local property of the local$ Opens key:

execution options

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

options\dllnxoptions

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

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

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

compatibility

Opens key: HKI M\

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:

HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration

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

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

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

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

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

Opens key:

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

 $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ policies\+ explorer$ Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer Opens key:

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

Opens kev:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ b9157 cdd 8f2376b26202 cce9b65f1efb. exemple \ begin{picture}$ 

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

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \clsid \closer{lem:hkcu} \end{tabular} $$ -20d04fe0-explorer \clsid \closer{lem:hkcu} \end{tabular} $$ -20d04fe0-explorer \clsid \closer{lem:hkcu} \end{tabular} $$ -20d04fe0-explorer \clsid \closer{lem:hkcu} \closer{l$ Opens key:

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

Opens key:

a2d8-08002b30309d}\shellfolder

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

Opens key:

 $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version\\| policies\\| none num between the content of the co$ 

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

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

08002b30309d}\inprocserver32

Opens key:

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

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2\ cpc \ volume \ \{d5291c64-7c88-4c40\} \ description \ de$ 

11e3-be65-806e6f6e6963}\

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

Opens key: HKCR\drive\shellex\folderextensions

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

4442-804e-409d6c4515e9}

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

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

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

97a27216f98a}\inprocserver32

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

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

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

Opens key: HKCR\folder

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

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:  ${\tt HKCU \backslash software \backslash classes \backslash directory \backslash browsein place}$ 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 kev: HKCR\folder\clsid

Opens key: HKCU\software\classes\allfilesystemobjects\clsid

Opens key: HKCR\allfilesystemobjects\clsid

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

a6bb2164fbd0}\inprocserver32

Opens key: HKLM\software\microsoft\com3

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

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

```
b8dc300d9f9d}
```

Opens key: HKCR\activatableclasses\clsid

Opens key: HKCR\activatableclasses\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
Opens key: HKCU\software\classes\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:  $\begin{tabular}{ll} HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas \\ Opens key: \\ HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc30d9f9d}\treatas \\ \begin{tabular}{ll} HKCU\software\clsid$ 

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:

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

Opens key:

 $\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \session in folders \end{tabular}$ 

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

folders

Opens key:

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

Opens key:

Opens key:

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

Opens key:

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

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-prop} $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}}$ 

Opens key:

 $\label{thm:local-state} $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}\property bag$ 

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

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

1923240461-1905901954-2556564120-1001

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:

 $\label{lem:hkculsoftware} HKCU software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ \{d5291c63-7c88-11e3-be65-806e6f6e6963\} \columnwidth \co$ 

Opens key: HKLM\software\wow6432node\propertycube

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

Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
Opens key: HKLM\system\currentcontrolset\control\nls\language groups

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ ctf \ compatibility \ b9157cdd8f2376b26202cce9b65f1efb. exemple \ description \$ 

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

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

 $Opens~key: \\ \qquad \qquad \text{HKLM} software \verb|microsoft| windows nt| current version \verb|| fontlink| systemlink| \\$ 

Opens key: HKLM\software\microsoft\windows

 $nt\current version\label{language} pack\datastore\_v1.0$ 

Opens key: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback Opens kev: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\ms shell dlg 2 Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty] Oueries value: HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback] HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type] Oueries value: Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\enus[alternatecodepage] Oueries value: HKCU\control panel\desktop[preferreduilanguages] HKCU\control panel\desktop\muicached[machinepreferreduilanguages] Queries value: Oueries value:  $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [prefer external manifest]$ HKLM\system\currentcontrolset\control\nls\sorting\versions[] Oueries value: Queries value: HKCU\software\microsoft\windows nt\currentversion\appcompatflags[showdebuginfo] HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Oueries value: HKLM\software\microsoft\windows nt\currentversion\image file execution Oueries value: options\dllnxoptions[usefilter] Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[b9157cdd8f2376b26202cce9b65f1efb.exe] Queries value: HKLM\software\microsoft\windows nt\currentversion\gre\_initialize[disablemetafiles] HKLM\software\wow6432node\microsoft\windows Oueries value: nt\currentversion\compatibility32[b9157cdd8f2376b26202cce9b65f1efb] HKLM\software\wow6432node\microsoft\windows Oueries value: nt\currentversion\windows[loadappinit\_dlls] Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled] Oueries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy] HKLM\software\microsoft\ole[pageallocatorusesystemheap] Queries value: Oueries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Queries value: HKLM\software\microsoft\ole[aggressivemtatesting] Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel] Queries value:  $HKLM \ software \ microsoft \ windows \ current version \ policies \ explorer [no set folders]$ HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us] Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx] Oueries 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] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 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]  $HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{20d04fe0-3aea-1069-a2d8-4069-a2d8$ 08002b30309d}] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\inprocserver32[] Queries value:  $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c64-7c88-4cq24, d544, d544,$ 11e3-be65-806e6f6e6963}[data] Oueries value:  $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c64-7c88-4cq24, d544, d544,$ 11e3-be65-806e6f6e6963}[generation] HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-Queries value: 409d6c4515e9}[drivemask] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden] HKCU\software\microsoft\windows\currentversion\explorer[shellstate] Oueries value: Oueries value: 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\currentversion\policies\explorer[nonetcrawling]
                                  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:
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| flide icons| \\ \end{tabular}
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
  Queries 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:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showstatusbar]
  Queries value:
                                  HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-
97a27216f98a}\inprocserver32[]
  Oueries value:
                                  HKCR\directory[docobject]
  Queries value:
                                  HKCR\folder[docobject]
  Queries value:
                                  HKCR\allfilesystemobjects[docobject]
  Queries value:
                                  HKCR\directory[browseinplace]
  Oueries value:
                                  HKCR\folder[browseinplace]
  Queries value:
                                  HKCR\allfilesystemobjects[browseinplace]
  Queries value:
                                  HKCR\directory[isshortcut]
  Oueries value:
                                  HKCR\folder[isshortcut]
                                  HKCR\allfilesystemobjects[isshortcut]
  Oueries value:
  Oueries 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[]
                                  HKLM\software\microsoft\com3[com+enabled]
  Queries value:
                                  HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
  Oueries value:
  Queries value:
                                  HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[inprocserver32]
                                  Oueries value:
b8dc300d9f9d}\inprocserver32[]
                                 HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
  Oueries value:
b8dc300d9f9d}\inprocserver32[threadingmodel]
                                  HKLM\software\microsoft\ole[maxsxshashcount]
  Oueries value:
  Oueries value:
db2c-424c-b029-7fe99a87c641}[category]
  Queries value:
db2c-424c-b029-7fe99a87c641}[name]
  Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ f
db2c-424c-b029-7fe99a87c641}[parentfolder]
  Oueries value:
db2c-424c-b029-7fe99a87c641}[description]
  Oueries value:
db2c-424c-b029-7fe99a87c641}[relativepath]
db2c-424c-b029-7fe99a87c641}[parsingname]
  Queries value:
db2c-424c-b029-7fe99a87c641}[infotip]
  Oueries value:
```

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

Oueries value:

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

Queries value:

 $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\gammable]$ 

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \begin{center} b4bfcc3a-db2c-424c-b029-7fe99a87c641 \stream \end{center} folder \descriptions \end{center} \label{lem:hklmsoftware} \label{lem:hklmsoftware}$ 

Queries value

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

folders[desktop]

Queries value:

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

Oueries value

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

Queries value:

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

Queries value:

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

Oueries value

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

Queries value:

Queries 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

b587-4786-b4ef-bd1dc332aeae}[roamable]

Oueries value:

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

Queries value:

 $H\dot{L}M\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[stream]

Queries value:

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

Oueries value:

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

Oueries value:

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

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folds 65f9-4cf6-a03a-e3ef65729f3d \cite{lem:hklmsoftware} \cite{lem:hklmsoftware} \end{substitute} The lem \cite{lem:hklmsoftware} \end{substitute} The lem \cite{lem:hklmsoftware} \cite{lem:hk$ 

Queries value:

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

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

Queries value:

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

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

folders[appdata]

Queries value:

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

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

Oueries value:

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

Oueries value:

 $HKLM \label{lem:hklm} Which was the statement of the st$ 0e22-4760-9afe-ea3317b67173}[description]

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

Oueries value:

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

Oueries value:

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

Queries value:

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

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

Queries value:

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

Oueries value:

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

Oueries value:

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

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

Queries value:

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

Oueries value:

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

Queries value:

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

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

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

Oueries value:

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

Oueries value:

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

HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

1923240461-1905901954-2556564120-1001[profileimagepath]

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

reporting\wmr[disable]

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

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c63-7c88-4cq24, d5291c63-7c88-4cq24, d5291c640-7c88-4cq24, d5291c64-7c88-4cq24, d5291c64-7c88-4cq24, d5291c64$ 11e3-be65-806e6f6e6963}[data]

Oueries value:

11e3-be65-806e6f6e6963}[generation]

HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]

Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000409] Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1] Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]

Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[scrollinset] Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]

Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist] Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[scrolldelay]

Queries value: HKCU\software\microsoft\windows

nt\currentversion\windows[scrollinterval]

Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\datastore\_v1.0[disable] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\datastore\_v1.0[datafilepath

nt\currentversion\languagepack\datastore\_v1.0[datafilepath]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]

Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane2] Queries value: HKLM\software\microsoft\windows

 $\label{lem:nt-current} $$ nt\circ \operatorname{languagepack} \sup_{t \in \mathbb{R}^{n}} \operatorname{languagepack} \operatorname{languagepac$ 

nt\currentversion\languagepack\surrogatefallback[plane4]
 Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]

Queries value: HKLM\software\microsoft\windows

 $\label{lem:nt-current-version-language} $$ \text{Queries value:} $$ \text{HKLM} \ \text{microsoft-windows} $$$ 

nt\currentversion\languagepack\surrogatefallback[plane7]
Queries value: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback[plane8] Queries value: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback[plane9]
Queries value: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback[plane10]
Queries value: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback[plane11]
Queries value: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback[plane12]

Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane13]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback[plane14]
Queries value: HKLM\software\microsoft\windows

 $\label{lem:nt-current-version-language-pack-surrogate-fall-back} \begin{tabular}{ll} $n \in \mathbb{N} \end{tabular} $$ \cline{15} \end{tabular} $$ Queries value: $$ HKLM\software\microsoft\windows $$ $$ \end{tabular} $$$ 

 $\verb|nt\currentversion\language| pack\surrogatefallback[plane16]|$