# Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 225, Task ID: 901

Task ID: 901

Risk Level: 4

Date Processed: 2016-04-28 13:12:22 (UTC)

Processing Time: 4.48 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\6d438b3e1ec4eca849107b093ce99dbc.exe"

Sample ID: 225 Type: basic Owner: admin

Label: 6d438b3e1ec4eca849107b093ce99dbc

Date Added: 2016-04-28 12:45:13 (UTC)

File Type: PE32:win32:gui File Size: 927416 bytes

MD5: 6d438b3e1ec4eca849107b093ce99dbc

SHA256: 9977dc742345ebc75d8914773e0af884e6ee16227f7acf9361fff7b681b971fc

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\6d438b3e1ec4eca849107b093ce99dbc.exe

["C:\windows\temp\6d438b3e1ec4eca849107b093ce99dbc.exe"]

Terminates process: C:\Windows\Temp\6d438b3e1ec4eca849107b093ce99dbc.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\nsmF5AA.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\nsiF761.tmp

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

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

Creates: C:\Users\Admin\AppData\Local\Temp\nsiF761.tmp\System.dll
Creates: C:\Users\Admin\AppData\Local\Temp\nsiF761.tmp\CityHash.dll
Opens: C:\Windows\Prefetch\6D438B3E1EC4ECA849107B093CE99-F2941E4F.pf

Opens: C:\Windows

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

Opens: C:\Windows\SysWOW64

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

Opens: C:\windows\temp\6d438b3e1ec4eca849107b093ce99dbc.exe.Local\

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

controls\_6595b64144ccf1df\_6.0.7601.17514\_none\_41e6975e2bd6f2b2

Opens: C:\Windows\winsxs\x86\_microsoft.windows.common-controls\_6595b64144ccf1df\_6.0.7601.17514\_none\_41e6975e2bd6f2b2\comctl32.dll

Opens: C:\windows\temp\VERSION.dll C:\Windows\SysWOW64\version.dll Opens: C:\Windows\SysWOW64\imm32.dll Opens: Opens: C:\Windows\WindowsShell.Manifest Opens: C:\Windows\SysWOW64\rpcss.dll Opens: C:\Windows\SysWOW64\uxtheme.dll Opens: C:\windows\temp\SHFOLDER.DLL  ${\tt C:\Windows\SysWOW64\shfolder.dll}$ Opens:

 ${\tt Opens:} \qquad {\tt C:\Windows\Globalization\Sorting\SortDefault.nls}$ 

Opens: C:\Windows\SysWOW64\shell32.dll

Opens: C:\

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

C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db Opens:

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

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

4C77-AF34-C647E37CA0D9}.1.ver0x00000000000001.db

C:\Users\Admin\Desktop\desktop.ini Opens: Opens: C:\windows\temp\profapi.dll Opens: C:\Windows\SysWOW64\profapi.dll C:\Users\Admin\AppData\Local\Temp Opens:

Opens: C:\Users\Admin\AppData\Local\Temp\nsmF5AA.tmp C:\Windows\Temp\6d438b3e1ec4eca849107b093ce99dbc.exe Opens:

C:\Windows\SysWOW64\en-US\setupapi.dll.mui Opens: Opens: C:\Users\Admin\AppData\Local\Temp\nsiF761.tmp

Opens: C:\Users Opens: C:\Users\Admin Opens: C:\Users\Admin\AppData Opens: C:\Users\Admin\AppData\Local

C:\Users\Admin\AppData\Local\Temp\nsiF761.tmp\System.dll Opens:

Opens: C:\Program Files (x86)

Opens: C:\Users\Admin\AppData\Local\Temp\nsiF761.tmp\CityHash.dll

Opens: C:\windows\temp\distribution\

Opens: C:\Windows\Temp

Writes to: C:\Users\Admin\AppData\Local\Temp\nsiF761.tmp\System.dll C:\Users\Admin\AppData\Local\Temp\nsiF761.tmp\CityHash.dll Writes to:

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

Reads from: C:\Windows\Temp\6d438b3e1ec4eca849107b093ce99dbc.exe Deletes: C:\Users\Admin\AppData\Local\Temp\nsmF5AA.tmp Deletes: C:\Users\Admin\AppData\Local\Temp\nsiF761.tmp

Deletes: C:\Users\Admin\AppData\Local\Temp\nsiF761.tmp\CityHash.dll C:\Users\Admin\AppData\Local\Temp\nsiF761.tmp\System.dll

## Windows Registry Events

Creates key: HKLM\software\wow6432node\mozilla\thunderbird\taskbarids

HKLM\software\wow6432node Creates key: Creates key: HKLM\software\wow6432node\mozilla

Creates key: HKLM\software\wow6432node\mozilla\thunderbird

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

options

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

HKLM\software\microsoft\wow64 Opens kev:

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

execution options

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

Opens kev:

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

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKLM\system\currentcontrolset\control\nls\customlocale

Opens key: HKLM\system\currentcontrolset\control\nls\language Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us

Opens key:  $\label{lem:hklmsystem} \verb|HKLM\| system \verb|\currentcontrolset\| control \verb|\mui\| uilanguages \verb|\pendingdelete|| \\$ 

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

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

Opens key:

Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration

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

Opens key: HKCU\control panel\desktop

HKCU\control panel\desktop\muicached Opens key:

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

Opens key:

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

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

HKLM\ Opens key:

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

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

nt\currentversion\gre\_initialize

Opens key:

 $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows$ 

nt\currentversion\compatibility32

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

compatibility

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

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

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

Opens key: Opens key:

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

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

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

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ 6d438b3e1ec4eca849107b093ce99dbc.exe$ 

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:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-

a2d8-08002b30309d}\shellfolder

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

Opens key:

 $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version\\| policies\\| nonenum$ 

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

Opens key:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \current version \explorer \mountpoints 2 \cpc \volume \end{tabular} \label{lem:hkcu}$ 

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}

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:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ shell \ registered applications \ urlass ociations \ directory \ open with progids \ not the shell \ registered \ not \$ 

Opens kev:

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

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

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

Opens key: HKCR\directory\curver Opens key: HKCR\directory\

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

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

Opens key: HKCR\folder

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

Opens key: HKCR\folder\shellex\iconhandler

Opens key: HKCU\software\classes\allfilesystemobjects

Opens key: HKCR\allfilesystemobjects

 $Opens~key: \\ \qquad \qquad \text{HKCU} software \verb|\classes| all filesystemobjects| shellex \verb|\iconhandler| \\$ 

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

 $Opens\ key: \\ HKCU \setminus software \setminus classes \setminus all filesystem objects \setminus browsein place$ 

Opens key: HKCR\allfilesystemobjects\browseinplace
Opens key: HKCU\software\classes\directory\clsid

Opens key: HKCR\directory\clsid

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

Opens key: HKCR\folder\clsid

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

Opens key: HKCR\allfilesystemobjects\clsid

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ \ folder descriptions$ 

Opens key:

db2c-424c-b029-7fe99a87c641}

Opens key:

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

db2c-424c-b029-7fe99a87c641}\propertybag

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus session in fo \setminus 1$ Opens kev:

Opens key:

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

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

folders

Opens kev: HKLM\software\microsoft\com3

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

b8dc300d9f9d}

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

b8dc300d9f9d}\treatas

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

b8dc300d9f9d}\progid

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

b8dc300d9f9d}\progid

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

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler

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

b8dc300d9f9d}\inprochandler

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

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

Opens key:

 $HKLM \label{lem:hklm} \\ \text{HKLM} \label{lem:hklm} wow 6432 node \label{lem:hklm} windows \label{lem:hklm} \\ \text{Lem:hklm} \label{lem:hklm} wow 6432 node \label{lem:hklm} \\ \text{HKLM} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \\ \text{HKLM} \label{lem:hklm} \label{lklm} \\ \text{HKLM} \label$ 

b587-4786-b4ef-bd1dc332aeae}

Opens key:

b587-4786-b4ef-bd1dc332aeae}\propertybag

65f9-4cf6-a03a-e3ef65729f3d}

Opens key:

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

Opens key:

0e22-4760-9afe-ea3317b67173}

Opens key:

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

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

nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001

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

980053277-1733835069-2361817685-1001

HKLM\system\currentcontrolset\control\cmf\config Opens key:

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

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

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

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

Opens key:  ${\tt HKLM \ } system \verb|\ current control \ \\ computer name \verb|\ active computer name \ \\$ Opens key: HKLM\system\setup

 ${\tt HKLM \ } . \\$ Opens key: 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:

11e3-a68e-806e6f6e6963}\

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

options\dllnxoptions

Opens key: HKLM\software\wow6432node\mozilla\thunderbird\taskbarids

HKCU\software\mozilla\thunderbird\taskbarids Opens key:

Opens key: HKLM\software

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

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

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

```
options[disableusermodecallbackfilter]
  Oueries value:
                                      HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
  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\en-
us[alternatecodepage]
  Oueries value:
                                      HKCU\control panel\desktop[preferreduilanguages]
  Queries value:
                                      HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Oueries value:
HKLM\svstem\currentcontrolset\control\nls\sorting\versions[]
  Oueries value:
  Queries value:
                                      HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:
                                      HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
                                      HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[6d438b3e1ec4eca849107b093ce99dbc]
  Queries value:
                                      HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:
                                      HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Oueries value:
                                      HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  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]
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
  Oueries value:
                                      HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Queries value:
                                      HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
  Oueries 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]
  Queries value:
                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsfordisplay]
  Queries value:
                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hidefolderverbs]
                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[usedrophandler]
                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[wantsforparsing]
                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
  Queries value:
                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforoverlay]
  Queries value:
                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[mapnetdriveverbs]
  Oueries value:
                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforinfotip]
                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[hideinwebview]
                                      Oueries value:
08002b30309d}\shellfolder[hideondesktopperuser]
  Queries value:
                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsaliasednotifications]
                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[wantsuniversaldelegate]
  Queries value:
                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[nofilefolderjunction]
                                      HKCR \setminus wow 6432 \\ node \\ \clsid \\ \cl
  Oueries value:
08002b30309d}\shellfolder[pintonamespacetree]
                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[hasnavigationenum]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d4-8213-
11e3-a68e-806e6f6e6963}[data]
```

Oueries value: 11e3-a68e-806e6f6e6963}[generation] HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-Queries value: 409d6c4515e9}[drivemask] Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden] HKCU\software\microsoft\windows\currentversion\explorer[shellstate] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]  $HKLM \verb|\software\microsoft\windows\currentversion\policies\explorer[separate process]|$ HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden] HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor] HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn] HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview] HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter] Oueries value: Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess] HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay] HKCR\directory[docobject] Queries value: Queries value: HKCR\folder[docobject] Queries value: HKCR\allfilesystemobjects[docobject] HKCR\directory[browseinplace] Oueries value: HKCR\folder[browseinplace] Queries value: HKCR\allfilesystemobjects[browseinplace] Oueries value: Queries value: HKCR\directory[isshortcut] Queries value: HKCR\folder[isshortcut] Queries value: HKCR\allfilesystemobjects[isshortcut] Queries value: HKCR\directory[alwaysshowext] Oueries value: HKCR\directory[nevershowext] Queries value: HKCR\folder[nevershowext] Queries value: HKCR\allfilesystemobjects[nevershowext] 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:

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

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:

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

Oueries value:

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

Oueries value

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value

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

Queries value:

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

Queries value:

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

Oueries value:

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

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

folders[desktop]

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

 $\label{lem:lem:queries value: HKCR\wow6432node\c1sid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\}[]} \\$ 

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\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:

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

Queries value:

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

Queries value

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

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:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value

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

Queries value:

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332eae\} \ [initfolder \ handler]$ 

 $\label{thm:condition} Queries \ value: \\ HKCU \ software \ \ microsoft \ \ windows \ \ current version \ \ explorer \ \ shell$ 

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value

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

Queries value:

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

Oueries value:

 $\label{lem:hklmsoftware} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[localized name]$ 

Queries value:

Queries value

 $\label{lem:hklmsoftware} HKLM software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1.5} \end{4.5} The des$ 

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value

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

Oueries value:

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

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]

Queries value: HKCU\software\microso

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:

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

Queries value:

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

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$ 

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

 $\label{lem:hklm} $HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[streamresource]$$ 

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

Oueries value

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[attributes]$ 

Queries value:

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

Queries value:

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

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

980053277-1733835069-2361817685-1001[profileimagepath]

Queries value: HKLM\system\currentcontrol\cmf\config[system]

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

reporting\wmr[disable]

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

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

Queries value:

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

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

Oueries value:

11e3-a68e-806e6f6e6963}[data]

Oueries value:

11e3-a68e-806e6f6e6963}[generation]

Queries value:

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

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

options\dllnxoptions[usefilter]

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

options\dllnxoptions[system.dll]

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

 $HKLM \ software \ wow 6432 node \ mozilla \ thunderbird \ taskbarids \ [c:\program]$ Sets/Creates value:

files (x86)\mozilla thunderbird]