# Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 185, Task ID: 740

Task ID: 740 Risk Level: 4

Date Processed: 2016-04-28 13:07:40 (UTC)

Processing Time: 2.86 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\2567808664106e29a8feaf65af1a22a6.exe"

Sample ID: 185 Type: basic Owner: admin

Label: 2567808664106e29a8feaf65af1a22a6

Date Added: 2016-04-28 12:45:09 (UTC)

File Type: PE32:win32:gui File Size: 119208 bytes

MD5: 2567808664106e29a8feaf65af1a22a6

SHA256: 0a6ca0d36bea70af831888244a384904a03772d3e33f63dd9c6b80f0e45d0d88

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\2567808664106e29a8feaf65af1a22a6.exe

["C:\windows\temp\2567808664106e29a8feaf65af1a22a6.exe"]

Terminates process: C:\Windows\Temp\2567808664106e29a8feaf65af1a22a6.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\nseD438.tmp

Creates: C:\Program Files
Creates: C:\Program Files\VuuPC

Opens: C:\Windows\Prefetch\2567808664106E29A8FEAF65AF1A2-45FF9F25.pf

Opens: C:\Windows\System32

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

Opens: C:\windows\temp\2567808664106e29a8feaf65af1a22a6.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 Opens: C:\Windows\System32\version.dll C:\Windows\System32\imm32.dll Opens: Opens: C:\Windows\WindowsShell.Manifest Opens: C:\Windows\System32\rpcss.dll Opens: C:\windows\temp\CRYPTBASE.dll Opens: C:\Windows\System32\cryptbase.dll Opens: C:\Windows\System32\uxtheme.dll Opens: C:\windows\temp\SHFOLDER.DLL C:\Windows\System32\shfolder.dll Opens:

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

Opens: C:\Windows\System32\shell32.dll

Opens: C:\

Opens: C:\Windows

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

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

Opens: C:\windows\temp\ntmarta.dll
Opens: C:\Windows\System32\ntmarta.dll

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

4C77-AF34-C647E37CA0D9}.1.ver0x000000000000006.db

Opens: C:\Windows\System32\en-US\setupapi.dll.mui

Opens: C:\Users\Admin\AppData\Local\Temp\nseD438.tmp
Opens: C:\Windows\Temp\2567808664106e29a8feaf65af1a22a6.exe

Opens: C:\Program Files
Opens: C:\Program Files\VuuPC

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

Reads from: C:\Windows\Temp\2567808664106e29a8feaf65af1a22a6.exe
Deletes: C:\Users\Admin\AppData\Local\Temp\nseD438.tmp

## Windows Registry Events

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

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

Opens key: HKCU\

Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration

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

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\microsoft\windows\currentversion\sidebyside

Opens key:

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

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

Opens key: HKLM\system\currentcontrolset\control\error message instrument\
Opens key: HKLM\system\currentcontrolset\control\error message instrument

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

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

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

Opens key: HKLM\

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

Opens key: HKLM\software\microsoft\ole

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

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

Opens key:

 $HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ applications \ \ 2567808664106e29a8 feaf 65af 1a22a6.exe$ 

Opens key: HKLM\software\microsoft\oleaut

Opens key: HKCU\software\classes\

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

08002b30309d}\shellfolder

Opens key: HKCR\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\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-

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

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

Opens key:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \mbox{$m$icrosoft \windows \current version \explorer \mbox{$m$ountpoints 2 \cpc \volume} \end{tabular} \label{lem:hkcu}$ 

Opens key:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mountpoints 2 \setminus cpc \setminus volume \setminus \{69d250e4-6c18-explorer\}$ 

11e3-b3bc-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\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:

 $\label{thm:local_equation} HKLM \software \microsoft \windows \shell \registered applications \urlass ociations \directory \label{thm:local_equations} \end{substitute} % \label{thm:local_equations} % \label{thm:loc$ 

Opens key:

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

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

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

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

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

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

Opens key: HKCR\folder

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

Opens key: HKCR\folder\shellex\iconhandler

Opens key: HKCU\software\classes\allfilesystemobjects

Opens key: HKCR\allfilesystemobjects

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

Opens key: HKCR\allfilesystemobjects\shellex\iconhandler Opens key: HKCU\software\classes\directory\docobject

Opens key: HKCR\directory\docobject

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

Opens key: HKCR\folder\docobject

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

Opens key: HKCR\allfilesystemobjects\docobject

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

Opens key: HKCR\directory\browseinplace

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

Opens key: HKCR\folder\browseinplace

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

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

Opens key: HKCR\directory\clsid

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

Opens key: HKCR\folder\clsid

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

Opens key: HKCR\allfilesystemobjects\clsid

Opens key:

 $\label{thm:local_hammon} \begin{tabular}{l} HKLM \end{tabular} software \end{tabular} in the constant \end{tabular} in the constant \end{tabular} and \end{tabular} in the constant \end$ 

Opens key:

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

Opens key:

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

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

Opens key:

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

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

folders

Opens key: HKLM\software\microsoft\com3

Opens key: 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

b8dc300d9f9d}\treatas

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

b8dc300d9f9d}\progid

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

b8dc300d9f9d}\inprocserver32

Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprochandler32

Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler

Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler
Opens key: HKLM\system\currentcontrolset\control\lsa\accessproviders

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

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

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

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

Opens key: HKLM\software\microsoft\rpc

Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername

Opens key: HKLM\system\setup

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

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

Opens key:

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

Opens kev:

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

Opens key:

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

Opens key:

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

Opens key:

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

Opens key:

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

Opens key:

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

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

2160590473-689474908-1361669368-1002

Opens kev:

 $\label{lem:hkcu} HKCU software \end{area} HKCU software \end{area} Less - 6c18-11e3-b3bc-806e6f6e6963 \end{area} Less - 6c18-12e3-b3bc-806e6f6e6963 \end{area}$ 

Opens key: HKLM\software\microsoft\rpc\extensions
Queries value: HKLM\system\currentcontrolset\control\session

manager[cwdillegalindllsearch]

Queries value:

 $HKLM \verb|\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]|$ 

Queries value: HKCU\control panel\desktop[preferreduilanguages]

Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]

Queries value:

HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]

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

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

nt\currentversion\compatibility32[2567808664106e29a8feaf65af1a22a6]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\windows[loadappinit\_dlls]

Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]

Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder[attributes]

Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder[callforattributes]

Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder[restrictedattributes]

Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder[wantsfordisplay]

Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder[hidefolderverbs]

Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder[usedrophandler]

Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder[wantsforparsing]

Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder[wantsparsedisplayname]

Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder[queryforoverlay]

Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[mapnetdriveverbs] Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[queryforinfotip] HKCR\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\shellfolder[hideinwebview] HKCR\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\shellfolder[hideondesktopperuser] HKCR\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\shellfolder[wantsaliasednotifications] HKCR\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\shellfolder[wantsuniversaldelegate] HKCR\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\shellfolder[nofilefolderjunction] Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[pintonamespacetree] HKCR\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\shellfolder[hasnavigationenum] Queries value: HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-08002b30309d}1 Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{69d250e4-6c18-11e3-b3bc-806e6f6e6963}[data] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{69d250e4-6c18-11e3-b3bc-806e6f6e6963}[generation] HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-Oueries value: 409d6c4515e9}[drivemask] Queries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons] Oueries 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: Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden] Oueries value: 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] Queries 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] Queries value: HKCR\directory[browseinplace] HKCR\folder[browseinplace] Queries value: Queries value: HKCR\allfilesystemobjects[browseinplace] HKCR\directory[isshortcut] Queries value: Oueries 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]

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}\cupreble{lem:hklmsoftware}\end{substitute}$ 

Oueries value:

Queries value:

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

Oueries value:

 $HKLM \ software \ microsoft \ \ current version \ \ explorer \ \ folder descriptions \ \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} \ [parent folder]$ 

Oueries value:

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

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} [relative path]$ 

Oueries value:

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

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \ \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} [infotip]$ 

Queries value:

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

Oueries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \ \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} \cite{ticon} \end{substitute}$ 

Queries value:

 $HKLM \ software \ microsoft \ \ current version \ \ explorer \ \ folder descriptions \ \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} [security]$ 

Oueries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \folds \current b029-7fe99a87c641 \subseteq \current \$ 

Oueries value:

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

Queries value:

 $HKLM \ software \ microsoft \ \ current version \ \ explorer \ \ folder descriptions \ \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} \ [local redirectonly]$ 

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \mbox{b4bfcc3a-db2c-424c-b029-7fe99a87c641} [stream]$ 

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \ \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} \ [publish expanded path]$ 

Queries value:

Oueries value:

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

Queries value:

HKLM\software\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]

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

b8dc300d9f9d}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[]

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

b8dc300d9f9d}\inprocserver32[threadingmodel]

Queries value: HKLM\software\microsoft\ole[maxsxshashcount]

Queries value:

 $HKLM \setminus system \setminus current control \\ \ \mid sa \setminus access providers \\ \ \mid marta extension \\ \ \mid sa \setminus access providers \\ \ \mid marta extension \\ \ \mid sa \setminus access providers \\ \ \mid marta extension \\ \ \mid sa \setminus access providers \\ \ \mid sa \setminus access providers$ 

Queries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
Queries value: HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
Queries value: HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]

Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]

Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]

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

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

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

Queries value:

HKLM\system\currentcontrolset\control\computername\activecomputername[computername]

Queries value: HKLM\system\setup[oobeinprogress]

Queries value: HKLM\system\setup[systemsetupinprogress]

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}\ [parsing name]$ 

Queries value:

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

Queries value:

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

Oueries value

Queries value:

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

Oueries value:

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

Queries value

 $HKLM \ software \ microsoft \ vurrent version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [stream resource type]$ 

Queries value:

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

Oueries value:

 $HKLM \ software \ microsoft \ vurrent version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [roamable]$ 

Queries value:

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

Queries value:

Queries value:

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

Queries value:

 $HKLM \ software \ microsoft \ \ current version \ \ explorer \ \ folder descriptions \ \ \ \ \ \ \ b4ef-bd1dc332aeae \ [attributes]$ 

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \end{area} \folder \fold$ 

Oueries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ folder descriptions \ `\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [init folder handler]$ 

Queries value:  $HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}]$ 

Queries value:

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

Queries value:

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

Queries value:

Oueries value:

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

Oueries value:

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

Oueries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{general} a03a-e3ef65729f3d \cal{general} [parsing name]$ 

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6a03a-e3ef65729f3d}[infotip]

Queries value:

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

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hklm} a03a-e3ef65729f3d \cal{lem:hklm} [icon]$ 

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{general} $\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [security] $\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \cal{hklk} $\{3eb685db-65f9-65f9-4cf6-a03a-e3ef65729f3d\} \cal{hklk} $\{3eb685db-65f9-65f9-65f6-a03a-e3ef65729f3d\} \cal{hklk} $\{3eb685db-65f9-65f9-65f6-a03a-e3$ 

Queries value:

 $\label{lem:hklm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[streamresource]$ 

Queries value:

Oueries value

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hklm} a03a-e3ef65729f3d \cal{lem:hklm} [publish expanded path]$ 

Oueries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-continuous} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \colored 3eb 685 db-65f9-4cf6-a03a-e3ef65729f3d \colored [initfolder handler]$ 

Queries value:

 $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}$ 

folders[appdata]

Queries value

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local_hklm} \begin{tabular}{l} HKLM \end{tabular} Software \end{tabular} in the constraint of the constrain$ 

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

 $HKLM \ software \ microsoft \ vurrent version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [icon]$ 

Oueries value:

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

Oueries value

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [stream resource]$ 

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value

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

Queries value:

 $HKLM \ software \ microsoft \ \ current version \ \ explorer \ \ folder descriptions \ \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [attributes]$ 

Oueries value:

 $HKLM \ software \ `microsoft \ `vindows \ current version \ explorer \ folder descriptions \ \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [folder type id]$ 

Queries value:

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

Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-2160590473-689474908-1361669368-1002[profileimagepath]

Queries value:

 $\label{lem:hkcu} HKCU software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \{69d250e3-6c18-11e3-b3bc-806e6f6e6963\} [data]$ 

Queries value

 $\label{lem:hkcu} HKCU software \end{area} In e3-b3bc-806e6f6e6963 \end{area} [generation]$ 

Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir]

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