# Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 135, Task ID: 541

Task ID: 541

Risk Level: 4

Date Processed: 2016-04-28 13:01:53 (UTC)

Processing Time: 2.66 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\2a154fe99ec69a4beb9bb9a0e38f7cee.exe"

Sample ID: 135 Type: basic Owner: admin

Label: 2a154fe99ec69a4beb9bb9a0e38f7cee

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

File Type: PE32:win32:gui File Size: 608199 bytes

MD5: 2a154fe99ec69a4beb9bb9a0e38f7cee

SHA256: b15518e358fb0663756ea1e0205603cec6304df6efaf4d08b08f112fe27a6c69

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\2a154fe99ec69a4beb9bb9a0e38f7cee.exe

["C:\windows\temp\2a154fe99ec69a4beb9bb9a0e38f7cee.exe"]

Terminates process: C:\Windows\Temp\2a154fe99ec69a4beb9bb9a0e38f7cee.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\nsu94D8.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\nsz94F8.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\nsz94F9.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\nsz94F9.tmp\nsHelper.dll
Opens: C:\Windows\Prefetch\2A154FE99EC69A4BEB9BB9A0E38F7-F91B6244.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\2a154fe99ec69a4beb9bb9a0e38f7cee.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:

Opens: 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:

C:\Windows\SysWOW64\en-US\setupapi.dll.mui Opens:

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

Opens:

4C77-AF34-C647E37CA0D9}.1.ver0x000000000000001.db

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

C:\Users\Admin\AppData\Local\Temp\nsu94D8.tmp Opens: Opens: C:\Windows\Temp\2a154fe99ec69a4beb9bb9a0e38f7cee.exe

Opens: C:\Users\Admin\AppData\Local\Temp\nsz94F9.tmp

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

C:\Users\Admin\AppData\Local\Temp\nsz94F9.tmp\nsHelper.dll Opens:

C:\Program Files (x86)\VideoSaver\ Opens: Opens: C:\Program Files (x86)\TubeSaver\

Writes to: C:\Users\Admin\AppData\Local\Temp\nsz94F8.tmp

C:\Users\Admin\AppData\Local\Temp\nsz94F9.tmp\nsHelper.dll Writes to:

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

C:\Windows\Temp\2a154fe99ec69a4beb9bb9a0e38f7cee.exe Reads from: Reads from: C:\Users\Admin\AppData\Local\Temp\nsz94F8.tmp Deletes: C:\Users\Admin\AppData\Local\Temp\nsu94D8.tmp Deletes: C:\Users\Admin\AppData\Local\Temp\nsz94F9.tmp

Deletes: C:\Users\Admin\AppData\Local\Temp\nsz94F9.tmp\nsHelper.dll

## Windows Registry Events

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

options

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

Opens key: HKLM\software\microsoft\wow64

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

execution options

Opens key: HKLM\system\currentcontrolset\control\safeboot\option Opens key: 

Opens key:

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

HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: 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: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete

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

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

Opens key: HKCU\

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

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

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

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

Opens key:

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

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

Opens key: HKLM\ Opens key:

HKLM\software\wow6432node\microsoft\windows nt\currentversion\diagnostics

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

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

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\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:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ 2a154 fe99ec69a4beb9bb9a0e38 f7cee. exemple \ applications \ applications$ 

Opens key: HKLM\software\wow6432node\microsoft\oleaut Opens key: HKCU\software\classes\

Opens key: HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder

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

08002b30309d}\shellfolder

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

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

Opens key:

a2d8-08002b30309d}\shellfolder

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

Opens key:

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

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

Opens key:

 $\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \end{tabular} \label{thm:linear}$ 

Opens key:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mountpoints 2 \setminus cpc \setminus volume \setminus \{8063a3d4-8213-mountpoints 2 \setminus cpc \setminus volume \setminus \{8063a3d4-8213-mountpoints 2 \setminus cpc \setminus volume \}$ 

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:

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:  ${\tt HKCU \setminus software \setminus classes \setminus all filesystem objects}$ 

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:  ${\tt HKCU \setminus software \setminus classes \setminus allfilesystemobjects \setminus clsid}$ 

Opens key: HKCR\allfilesystemobjects\clsid

Opens key:

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

 $HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$ 

db2c-424c-b029-7fe99a87c641}

Opens key:

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

 $Opens~key: \\ HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in following the context of the co$ 

Opens key:

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

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

folders

Opens key: HKLM\software\microsoft\com3

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

b8dc300d9f9d}

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

b8dc300d9f9d}\treatas

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

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

b8dc300d9f9d}\progid

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

b8dc300d9f9d}\progid

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

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler

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

b8dc300d9f9d}\inprochandler

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

Opens key: HKLM\software\www6432node\microsoft\windows\windows error reporting\wmr
Opens key: HKLM\software\www6432node\microsoft\windows\currentversion\setup

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

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

Opens key: HKLM\system\currentcontrol\computername\activecomputername

Opens key: HKLM\system\setup

Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc

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

Opens key: HKLM\software\microsoft\sqmclient\windows
Opens key: HKLM\system\currentcontrol\set\control\lsa\accessproviders

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

Opens key:

 $\label{lem:hklm} \begin{tabular}{ll} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings Opens key: \end{tabular}$ 

Opens key:

Opens key:

Opens key:

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

Opens key:

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

Opens key:

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

Opens key:

 $\label{thm:local-bound} HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ \{8063a3d3-8213-11e3-a68e-806e6f6e6963\} \label{thm:local-bound}$ 

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

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

settings Opens key:

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

settings

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

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

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

options[disableusermodecallbackfilter]

Queries value: HKLM\system\currentcontrolset\control\session

manager[cwdillegalindllsearch]

Queries value:

```
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
   Oueries value:
                                              HKLM\system\currentcontrolset\control\nls\customlocale[empty]
   Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
                                              HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
   Queries value:
   Queries value:
                                               HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
                                               HKCU\control panel\desktop[preferreduilanguages]
   Queries value:
   Oueries value:
                                              HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
   Oueries value:
                                              HKLM\svstem\currentcontrolset\control\nls\sorting\versions[]
   Queries value:
                                              HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
                                              HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\gre_initialize[disablemetafiles]
                                              HKLM\software\wow6432node\microsoft\windows
   Oueries value:
nt\currentversion\compatibility32[2a154fe99ec69a4beb9bb9a0e38f7cee]
   Queries value:
                                              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit dlls]
                                              HKLM\software\microsoft\ole[pageallocatorusesystemheap]
   Oueries value:
                                              HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
   Oueries value:
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
   Oueries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:local_hammon} software \end{tabular} in the internetion \end{tabular} and \begin{tabular}{ll} help the internetion \end{tabular} and \begin{tabular
   Queries value:
                                               HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
   Oueries value:
                                              HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
                                              Oueries value:
08002b30309d}\shellfolder[attributes]
                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[callforattributes]
   Oueries value:
                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[restrictedattributes]
   Queries value:
                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsfordisplay]
                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[hidefolderverbs]
   Queries value:
                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[usedrophandler]
   Queries value:
                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsforparsing]
                                              Oueries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[queryforoverlay]
                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[mapnetdriveverbs]
   Queries value:
                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforinfotip]
   Queries value:
                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideinwebview]
                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[hideondesktopperuser]
                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[wantsuniversaldelegate]
   Queries value:
                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[nofilefolderjunction]
                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[pintonamespacetree]
                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[hasnavigationenum]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}1
   Queries value:
11e3-a68e-806e6f6e6963}[data]
   Queries value:
11e3-a68e-806e6f6e6963}[generation]
                                              HKCR \ drive \ bellex \ folder extensions \ \{fbeb8a05-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4446-beee-4446-beee-4446-beee-4446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-
   Oueries value:
```

409d6c4515e9}[drivemask] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden] HKCU\software\microsoft\windows\currentversion\explorer[shellstate] Queries value: Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview] Oueries 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] HKLM\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext] HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath] HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip] Queries 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] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect] HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay] Queries value: HKCR\directory[docobject] HKCR\folder[docobject] Oueries value: Oueries value: HKCR\allfilesystemobjects[docobject] Queries value: HKCR\directory[browseinplace] Queries value: HKCR\folder[browseinplace] Queries value: HKCR\allfilesystemobjects[browseinplace] Oueries value: HKCR\directory[isshortcut] HKCR\folder[isshortcut] Oueries value: HKCR\allfilesystemobjects[isshortcut] Queries value: Oueries value: HKCR\directory[alwaysshowext] Queries value: HKCR\directory[nevershowext] Queries value: HKCR\folder[nevershowext] Queries value: HKCR\allfilesystemobjects[nevershowext] db2c-424c-b029-7fe99a87c641}[category] Oueries value:  $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ f$ db2c-424c-b029-7fe99a87c641}[name] Oueries value: db2c-424c-b029-7fe99a87c641}[parentfolder] Queries value: db2c-424c-b029-7fe99a87c641}[description]  $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{b4bfcc3a-b4bf$ db2c-424c-b029-7fe99a87c641}[relativepath] Queries value: db2c-424c-b029-7fe99a87c641}[parsingname] Oueries value: db2c-424c-b029-7fe99a87c641}[infotip]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-

Oueries value:

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

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

Queries value:

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

Queries value:

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

Oueries value

 $\label{thm:local-state} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma\g$ 

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value

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

Queries value:

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

Oueries 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:

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

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

folders[desktop]

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

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

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

b8dc300d9f9d}\inprocserver32[inprocserver32]

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

b8dc300d9f9d}\inprocserver32[]

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

b8dc300d9f9d}\inprocserver32[threadingmodel]

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

 $\label{lem:lem:queries} Queries \ value: HKLM\system\currentcontrolset\control\cmf\config[system] \\ HKLM\software\wow6432node\microsoft\windows\windows\ error \\ \end{tabular}$ 

reporting\wmr[disable]

 $\label{lem:queries value: Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath] \\ \mbox{Queries value: } HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath] \\ \mbox{}$ 

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]

Oueries 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{thm:local-basis} $$HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[category]$$ 

Queries value:

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

Oueries value

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

Queries value:

Queries value:

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

Queries value:

 $\label{thm:local-basis} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1} b587-4786-b4ef-bd1dc332 aeae \cite{1} [parsing name]$ 

Oueries value:

 $\label{thm:local-continuous} HKLM \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} wow 6432 node \end{tabular} microsoft \end{tabular} windows \end{tabular} \begin{tabular}{ll} HKLM \e$ 

b587-4786-b4ef-bd1dc332aeae}[infotip]

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries 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

 $\label{local-basis} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f(1b3ea5dc-b587-4786-b4ef-bd1dc332aeae)\cite{Common-c$ 

Queries 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:

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

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:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value

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

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value

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

Oueries value

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

Oueries value:

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

Oueries value:

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

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[appdata]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

Oneries value

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value

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

Queries value:

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

Oueries value:

 $\label{thm:local-ham} $HKLM \sim \text{$000} $$ HKLM \sim \text{$0000} $$ HKLM \sim \text{$0000} $$ HKLM \sim \text{$0000} $$ HKLM \sim \text{$0000} $$ H$ 

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1.5} Ge6c858f-0e22-4760-9 af e-ea3317b67173 \finit folder handler]$ 

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

980053277-1733835069-2361817685-1001[profileimagepath]

Queries value:

 $\label{thm:local-bound} HKCU software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ \{8063a3d3-8213-11e3-a68e-806e6f6e6963\} \cite{Absolution} \cite{Absolution}$ 

Queries value:

 $HKCU \ software \ `microsoft \ `windows \ current version \ explorer \ `mountpoints2 \ cpc \ volume \ \{8063a3d3-8213-11e3-a68e-806e6f6e6963\} \ [generation]$ 

Queries value:

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

Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings[disableimprovedzonecheck]

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

settings[security\_hklm\_only]

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