Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 135, Task ID: 540

Task ID: 540 Risk Level: 4

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

Processing Time: 2.72 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\nsnBD91.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\nsnBD9C.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\nsxBDA7.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\nsxBDA7.tmp\nsHelper.dll
Opens: C:\Windows\Prefetch\2A154FE99EC69A4BEB9BB9A0E38F7-F91B6244.pf

Opens: C:\Windows\System32

Opens: C:\Windows\System32\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

C:\windows\temp\VERSION.dll Opens: Opens: C:\Windows\System32\version.dll Opens: C:\Windows\System32\imm32.dll 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 C:\windows\temp\SHFOLDER.DLL Opens: Opens: C:\Windows\System32\shfolder.dll

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

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

Opens: C:\

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

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:\Users\Admin\AppData\Local\Temp
Opens: C:\Users\Admin\AppData\Local\Temp\nsdBD91.tmp
Opens: C:\Windows\Temp\2a154fe99ec69a4beb9bb9a0e38f7cee.exe

Opens: C:\Users\Admin\AppData\Local\Temp\nsxBDA7.tmp

Opens: C:\Users
Opens: C:\Users\Admin

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

Opens: C:\Users\Admin\AppData\Local\Temp\nsxBDA7.tmp\nsHelper.dll

Opens: C:\Program Files\VideoSaver\
Opens: C:\Program Files\TubeSaver\

Writes to: C:\Users\Admin\AppData\Local\Temp\nsnBD9C.tmp

 $\label{local-loc$

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

Reads from: C:\Windows\Temp\2a154fe99ec69a4beb9bb9a0e38f7cee.exe
Reads from: C:\Users\Admin\AppData\Local\Temp\nsnBD9C.tmp
Deletes: C:\Users\Admin\AppData\Local\Temp\nsdBD91.tmp
Deletes: C:\Users\Admin\AppData\Local\Temp\nsxBDA7.tmp

Deletes: C:\Users\Admin\AppData\Local\Temp\nsxBDA7.tmp\nsHelper.dll

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:

 $HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ applications \ 2a154fe99ec69a4beb9bb9a0e38f7cee. exemple \ descriptions \ and \ applications \ applicati$

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:

Opens key:

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

 $Opens~key: \\ HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus advanced$

Opens key:

 $HKLM \ software \ microsoft \ windows \ shell \ registered applications \ urlassociations \ directory \ open with progids$

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

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

Opens key: HKCR\directory\docobject

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

Opens key: HKCR\folder\docobject

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

Opens key: HKCR\allfilesystemobjects\docobject

Opens key: ${\tt HKCU \setminus software \setminus classes \setminus directory \setminus browseinplace}$

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: 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:

 $\label{thm:local_hammon} HKLM \label{thm:local_hammon} HKLM \label{thm:local_hammon} which is a substitution of the local hammon \label{thm:local_hammon} HKLM \label{thm:local_hammon}.$

Opens key:

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

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:

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

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

Opens key:

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

b8dc300d9f9d}\progid

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

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\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:

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

Opens key:

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

Opens key:

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

Opens key:

 $HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}\propertybag$

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

2160590473-689474908-1361669368-1002

Opens key:

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

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

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

settings

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

manager[cwdillegalindllsearch]

Queries value:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [transparent enabled]$

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[2a154fe99ec69a4beb9bb9a0e38f7cee]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\windows[loadappinit_dlls]

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

HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Oueries value: 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] Oueries 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] HKCR\clsid\{20d04fe0-3aea-1069-a2d8-Queries value: 08002b30309d}\shellfolder[wantsforparsing] HKCR\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\shellfolder[wantsparsedisplayname] Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[queryforoverlay] HKCR\clsid\{20d04fe0-3aea-1069-a2d8-Queries value: 08002b30309d}\shellfolder[mapnetdriveverbs] Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[queryforinfotip] Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[hideinwebview] Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[hideondesktopperuser] Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsaliasednotifications] Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsuniversaldelegate] Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[nofilefolderjunction] HKCR\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\shellfolder[pintonamespacetree] Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\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\{69d250e4-6c18-11e3-b3bc-806e6f6e6963}[data] HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{69d250e4-6c18-11e3-b3bc-806e6f6e6963}[generation] HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-Queries value: 409d6c4515e9}[drivemask] Queries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor] 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] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter] 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]

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]

Queries value: HKCR\directory[docobject]
Queries value: HKCR\folder[docobject]

Queries value: HKCR\allfilesystemobjects[docobject]
Queries value: HKCR\directory[browseinplace]

Queries value: HKCR\folder[browseinplace]

Queries value: HKCR\allfilesystemobjects[browseinplace]

Queries value: HKCR\directory[isshortcut]
Queries value: HKCR\folder[isshortcut]

Queries value: HKCR\allfilesystemobjects[isshortcut]

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

Queries value: HKLM\software\microsoft\windows\error reporting\wmr[disable]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
Queries value: HKLM\software\microsoft\windows\currentversion[devicepath]

Queries value: HKCR\directory[alwaysshowext]
Queries value: HKCR\directory[nevershowext]
Queries value: HKCR\folder[nevershowext]

Queries value: HKCR\allfilesystemobjects[nevershowext]

Queries value:

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

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:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}[security]$

Queries value:

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

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

Queries value:

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

Queries value:

 $\label{thm:microsoft} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}[localredirectonly]}$

Oueries value

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

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ microsoft \ \ current version \ \ explorer \ \ folder descriptions \ \ \ \ \ b029-7fe99a87c641 \ [publish expanded path]$

Oueries value:

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

Oueries value:

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

Oueries 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}[]

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\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:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \current b4ef-bd1dc332aeae \current \current$

Queries value:

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

Queries value:

Oueries value:

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

Queries value:

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

Queries value

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

Oueries value:

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

Queries value:

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

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

Oueries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \calebox{3eb685db-65f9-4cf6-a03a-e3ef65729f3d} \category\cite{Control of the control of the control$

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value

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

Queries value:

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

Oueries 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{lem:hklm} a03a-e3ef65729f3d \security \$

Oueries value:

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

Queries value:

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

Oueries value:

 $\label{lem:hklm} \begin{tabular}{l} HKLM \end{tabular} windows \current version \explorer \folder descriptions \end{tabular} \begin{tabular}{l} 43eb685db-65f9-4cf6-a03a-e3ef65729f3d \end{tabular} \begin{tabular}{l} 10cal redirection \end{tabular} \begin{tabular}{l} 10cal red in the constraint \end{tabular} \begin{tabular}{l} 10cal$

Queries value:

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

Queries value:

Queries value:

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

Oueries value:

 $HKLM \ software \ microsoft \ \ current version \ \ explorer \ \ folder descriptions \ \ \ \ a03a-e3ef65729f3d \ [publish expanded path]$

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{general} a 03a-e3ef65729f3d \end{general} [attributes]$

Queries value:

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

Queries value:

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

Queries value:

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

folders[appdata]

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value

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

Queries value:

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

Oueries value:

 $\label{local-observation} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \folder \folder$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

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

Oueries value

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

Queries value:

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

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

Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]

Queries value: HKLM\software\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]