# Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 246, Task ID: 984

Task ID: 984 Risk Level: 7

Date Processed: 2016-04-28 13:14:19 (UTC)

Processing Time: 2.95 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\280c53057f49089a8bbef69fce3e81cd.exe"

Sample ID: 246 Type: basic Owner: admin

Label: 280c53057f49089a8bbef69fce3e81cd

Date Added: 2016-04-28 12:45:15 (UTC)

File Type: PE32:win32:gui File Size: 376040 bytes

MD5: 280c53057f49089a8bbef69fce3e81cd

SHA256: dcf31db18983784dcecab6c4557722cb32cc384121b5b4cc77930b071f747c25

Description: None

### Pattern Matching Results

7 Signed by adware producer [Adware, PUA]

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\280c53057f49089a8bbef69fce3e81cd.exe

["C:\windows\temp\280c53057f49089a8bbef69fce3e81cd.exe"]

Terminates process: C:\Windows\Temp\280c53057f49089a8bbef69fce3e81cd.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\

 $\label{lem:condition} Creates: $$C:\Users\land Admin\land AppData\land Local\land Temp\land SFOBC.tmp $$C:\Users\land Admin\land AppData\land Local\land Temp\land SF171.tmp $$$ 

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

Creates: C:\Users\Admin\AppData\Local\Temp\nswF171.tmp\tkDecript.dll
Creates: C:\Users\Admin\AppData\Local\Temp\nswF171.tmp\version.dll
Opens: C:\Windows\Prefetch\280C53057F49089A8BBEF69FCE3E8-6305A30E.pf

Opens: C:\Windows\System32

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

Opens: C:\windows\temp\280c53057f49089a8bbef69fce3e81cd.exe.Local\

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

controls\_6595b64144ccf1df\_5.82.7601.17514\_none\_ec83dffa859149af

Opens: C:\Windows\winsxs\x86\_microsoft.windows.common-controls\_6595b64144ccf1df\_5.82.7601.17514\_none\_ec83dffa859149af\comctl32.dll

Opens: C:\windows\temp\VERSION.dll
Opens: C:\windows\System32\version.dll
Opens: C:\windows\System32\apphelp.dll
Opens: C:\windows\AppPatch\sysmain.sdb

Opens: C:\Windows\Temp\280c53057f49089a8bbef69fce3e81cd.exe

C:\Windows\System32\uxtheme.dll Opens: C:\windows\temp\WINMM.dll Opens: Opens: C:\Windows\System32\winmm.dll Opens: C:\windows\temp\samcli.dll C:\Windows\System32\samcli.dll Opens: Opens: C:\windows\temp\MSACM32.dll C:\Windows\System32\msacm32.dll Opens: Opens: C:\windows\temp\sfc.dll Opens: C:\Windows\System32\sfc.dll C:\windows\temp\sfc\_os.DLL Opens: Opens: C:\Windows\System32\sfc\_os.dll Opens: C:\windows\temp\USERENV.dll Opens: C:\Windows\System32\userenv.dll Opens: C:\windows\temp\profapi.dll Opens: C:\Windows\System32\profapi.dll Opens: C:\windows\temp\dwmapi.dll Opens: C:\Windows\System32\dwmapi.dll C:\windows\temp\MPR.dll Opens: Opens: C:\Windows\System32\mpr.dll Opens: C:\windows\temp\280c53057f49089a8bbef69fce3e81cd.exe.Manifest Opens: C:\Windows\System32\imm32.dll Opens: C:\Windows\System32\en-US\setupapi.dll.mui Opens: C:\Windows\System32\rpcss.dll C:\windows\temp\CRYPTBASE.dll Opens: Opens: C:\Windows\System32\cryptbase.dll Opens: C:\windows\temp\SHFOLDER.DLL Opens: C:\Windows\System32\shfolder.dll Opens: C:\Windows\Globalization\Sorting\SortDefault.nls Opens: C:\Windows\System32\shell32.dll Opens: C:\Windows\winsxs\x86\_microsoft.windows.commoncontrols\_6595b64144ccf1df\_6.0.7601.17514\_none\_41e6975e2bd6f2b2 Opens: C:\Windows\winsxs\x86\_microsoft.windows.commoncontrols\_6595b64144ccf1df\_6.0.7601.17514\_none\_41e6975e2bd6f2b2\comctl32.dll Opens: C:\Windows\WindowsShell.Manifest 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 C:\Windows\System32\ntmarta.dll Opens:

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

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

Opens: C:\Users\Admin\Desktop\desktop.ini Opens: C:\Users\Admin\AppData\Local\Temp

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

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

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

Opens: C:\Users\Admin\AppData\Local\Temp\nswF171.tmp

Opens: C:\Users\Admin\AppData\Local\Temp\nswF171.tmp\tkDecript.dll Opens: C:\Users\Admin\AppData\Local\Temp\nswF171.tmp\version.dll Writes to: C:\Users\Admin\AppData\Local\Temp\nswF171.tmp\tkDecript.dll Writes to: C:\Users\Admin\AppData\Local\Temp\nswF171.tmp\version.dll

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

C:\Windows\Temp\280c53057f49089a8bbef69fce3e81cd.exe Reads from:

C:\Users\Admin\AppData\Local\Temp\nsyFOBC.tmp Deletes: Deletes: C:\Users\Admin\AppData\Local\Temp\nswF171.tmp

C:\Users\Admin\AppData\Local\Temp\nswF171.tmp\tkDecript.dll Deletes: Deletes: C:\Users\Admin\AppData\Local\Temp\nswF171.tmp\version.dll

## Windows Registry Events

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

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

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

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

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

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

Opens key:

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

Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions

Opens key: HKLM\software\policies\microsoft\windows nt\windows file protection
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\oleaut

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

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\system\currentcontrolset\control\networkprovider\hworder
Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer

Opens key:

 $HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ applications \ 280c53057f49089a8bbef69fce3e81cd. exemple \ applications \$ 

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

 $Opens~key: \\ HKCU software \microsoft \windows \current version \explorer \clsid \ \{20d04feo-defined and the context of the$ 

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:

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

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\software\microsoft\windows\currentversion\explorer\advanced

Opens key:

Opens key:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU software \verb|\microsoft| windows \verb|\shell| associations \verb|\urlassociations| directory \\ \begin{tabular}{ll} HKCU software \verb|\microsoft| windows \verb|\shell| associations \verb|\urlassociations| directory \\ \begin{tabular}{ll} HKCU software \verb|\microsoft| windows \verb|\shell| associations \\ \begin{tabular}{ll} HKCU software \verb|\microsoft| windows \verb|\shell| associations \\ \begin{tabular}{ll} HKCU software \verb|\microsoft| windows \\ \begin{tabular}{ll} HKCU software \verb|\microsoft| windows \\ \begin{tabular}{ll} HKCU software \\ \begin{tabular}$ 

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  ${\tt HKCR\allfilesystemobjects\shellex\iconhandler}$ Opens key: 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 HKCU\software\classes\allfilesystemobjects\clsid Opens key: Opens key: HKCR\allfilesystemobjects\clsid Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions Opens key: b029-7fe99a87c641} Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}\propertybag  $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus session in four themselves the following of the follow$ Opens kev: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders Opens 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-8f50b8dc300d9f9d}\treatas HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\progid HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid Opens key: Opens key: HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\inprocserver32 HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32 Opens key: Opens key: HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\inprochandler32 HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler32 Opens key:

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:

 $\label{lem:hklm} \mbox{\tt HKLM} software \verb|\mbox{\tt microsoft}| windows \verb|\currentversion| explorer \verb|\knownfoldersettings| | \mbox{\tt microsoft}| \mbox{\tt microsoft}|$ 

Opens key:

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

Opens key:

 $HKLM \ software \ microsoft \ vurrent version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} \ property bag$ 

Opens key:

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

Opens key:

 $\label{lem:hkklm} HKLM software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hkklm} a 03a-e3ef65729f3d \property bag$ 

Opens key:

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

Opens key:

 $HKLM \setminus software \setminus irrestant + software \setminus ir$ 

9afe-ea3317b67173}\propertybag

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

2160590473-689474908-1361669368-1002

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:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mountpoints 2 \setminus cpc \setminus volume \setminus \{69d250e3-6c18-160d20e3-6c18-160d20e3-6c18-160d20e3-6c18-160d20e3-6c18-160d20e3-6c18-160d20e3-6c18-160d20e3-6c18-160d20e3-6c18-160d20e3-6c18-160d20e3-6c18-160d20e3-6c18-160d20e3-6c18-160d20$ 

11e3-b3bc-806e6f6e6963}\

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

options

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

options\dllnxoptions

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

manager[cwdillegalindllsearch]

Queries value:

HKLM\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: HKCU\software\microsoft\windows

nt\currentversion\appcompatflags[showdebuginfo]

Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value: HKLM\software\policies\microsoft\windows nt\windows file

protection[knowndlllist]

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[280c53057f49089a8bbef69fce3e81cd]

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\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\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
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: 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]

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

08002b30309d}\shellfolder[hideinwebview]

```
HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
 Oueries value:
08002b30309d}\shellfolder[hideondesktopperuser]
                          HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries 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]
 Oueries value:
                          HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[pintonamespacetree]
                          HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
 Oueries value:
08002b30309d}\shellfolder[hasnavigationenum]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}]
 Queries 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-
 Queries value:
409d6c4515e9}[drivemask]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
 Queries value:
Oueries value:
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]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
                          HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
 Oueries value:
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
 Queries 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]
 Queries value:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced| [showtypeoverlay] \\ \end{tabular}
 Oueries value:
                          HKCR\directory[docobject]
 Queries value:
                          HKCR\folder[docobject]
 Queries value:
                          HKCR\allfilesystemobjects[docobject]
 Queries value:
                          HKCR\directory[browseinplace]
 Oueries value:
                          HKCR\folder[browseinplace]
 Queries value:
                          HKCR\allfilesystemobjects[browseinplace]
 Queries value:
                          HKCR\directory[isshortcut]
 Queries value:
                          HKCR\folder[isshortcut]
 Queries value:
                          HKCR\allfilesystemobjects[isshortcut]
 Queries value:
                          HKCR\directory[alwaysshowext]
                          HKCR\directory[nevershowext]
 Queries value:
 Queries value:
                          HKCR\folder[nevershowext]
 Queries value:
                          HKCR\allfilesystemobjects[nevershowext]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[category]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[name]
 Oueries value:
```

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-

b029-7fe99a87c641}[parentfolder]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[description]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[relativepath]

Oueries value:

b029-7fe99a87c641}[parsingname]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[infotip]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[localizedname]

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[icon]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[security]

Oueries value:

b029-7fe99a87c641}[streamresource]

Queries value:

b029-7fe99a87c641}[streamresourcetype]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[localredirectonly]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[roamable]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[precreate]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[stream]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[publishexpandedpath]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[attributes]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[foldertypeid]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[initfolderhandler]

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

folders[desktop]

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

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[]

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

b8dc300d9f9d}\inprocserver32[threadingmodel]

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

Queries value:

HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]

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

HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]

Oueries value:

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

Oueries value:

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

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-

b4ef-bd1dc332aeae}[parentfolder]

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value

 $\label{thm:local-continuous} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \eqref{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae} [init folder \handler]$ 

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

Queries value:

 $\label{lem:hklm} \begin{tabular}{ll} HKLM \end{tabular} $$HKLM \end{tabular} $$ HKLM \$ 

Queries value:

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

Queries value:

Queries value:

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

Oueries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \eqref{3eb685db-65f9-4cf6-a03a-e3ef65729f3d} \cite{1.0cm} \$ 

Queries value:

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

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-

a03a-e3ef65729f3d}[infotip]

Queries value:

 $HKLM \ software \ microsoft \ \ current version \ \ explorer \ \ folder descriptions \ \ \ \ \ a03a-e3ef65729f3d \ [localized name]$ 

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

 $HKLM \ software \ microsoft \ \ current version \ \ explorer \ \ folder descriptions \ \ \ \ a03a-e3ef65729f3d \ [init folder handler]$ 

Queries value:

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

folders[appdata]

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-

9afe-ea3317b67173}[streamresource]

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value

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

Queries value:

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

Queries value:

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

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

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:

 $\label{lem:hkcu} HKCU software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ \{69d250e3-6c18-11e3-b3bc-806e6f6e6963\} \cline{200} \$ 

Queries value:

 $\label{thm:local-continuous} HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \end{69d250e3-6c18-11e3-b3bc-806e6f6e6963} \end{69d250e3-6c18-11e3-b3bc-806e6f6e69696} \end{69d250e3-6c18-11e3-b3bc-806e6f6e696969} \end{69d250e3-6c18-11e3-b3bc-806e6f6e6969} \end{69d250e3-6c18-11e3-b3bc-806e6f6e69696} \end{69d250e3-6c18-11e3-006e6f6e6969} \end{69d250e3-6c18-11e3-006e6f6e6969} \end{69d250e3-6c18-11e3-0$ 

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[usefilter]

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[version.dll]

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