Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	872
Risk Level:	4
Date Processed:	2016-04-28 13:11:41 (UTC)
Processing Time:	2.66 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	`"c:\windows\temp\afdd75bce006a193064e6227738b4bea.exe"`
Sample ID:	218
Type:	basic
Owner:	admin
Label:	afdd75bce006a193064e6227738b4bea
Date Added:	2016-04-28 12:45:12 (UTC)
File Type:	PE32:win32:gui
File Size:	176199 bytes
MD5:	afdd75bce006a193064e6227738b4bea
SHA256:	03f36b2c7ea1856849d6a32ee216580778c34f95d50cdf6a1a9af3f37087aaf9
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\afdd75bce006a193064e6227738b4bea.exe`
`["C:\windows\temp\afdd75bce006a193064e6227738b4bea.exe" ]`	
Terminates process:	`C:\Windows\Temp\afdd75bce006a193064e6227738b4bea.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\nsdD777.tmp`
Opens:	`C:\Windows\Prefetch\AFDD75BCE006A193064E6227738B4-26AA02F1.pf`
Opens:	`C:\Windows\System32`
Opens:	`C:\Windows\System32\sechost.dll`
Opens:	`C:\windows\temp\afdd75bce006a193064e6227738b4bea.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\imm32.dll`
Opens:	`C:\Windows\System32\rpcss.dll`
Opens:	`C:\windows\temp\CRYPTBASE.dll`
Opens:	`C:\Windows\System32\cryptbase.dll`
Opens:	`C:\Windows\System32\uxtheme.dll`
Opens:	`C:\windows\temp\SHFOLDER.DLL`
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.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\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
  Opens:                    C:\Windows\System32\ntmarta.dll
  Opens:                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000006.db
  Opens:                    C:\Users\Admin\Desktop\desktop.ini
  Opens:                    C:\Windows\System32\en-US\setupapi.dll.mui
  Opens:                    C:\windows\temp\profapi.dll
  Opens:                    C:\Windows\System32\profapi.dll
  Opens:                    C:\Users\Admin\AppData\Local\Temp
  Opens:                    C:\Users\Admin\AppData\Local\Temp\nsdD777.tmp
  Opens:                    C:\Windows\Temp\afdd75bce006a193064e6227738b4bea.exe
  Reads from:               C:\Users\Admin\Desktop\desktop.ini
  Reads from:               C:\Windows\Temp\afdd75bce006a193064e6227738b4bea.exe
  Deletes:                  C:\Users\Admin\AppData\Local\Temp\nsdD777.tmp
```

Windows Registry Events

```
  Opens key:            HKLM\system\currentcontrolset\control\session manager
  Opens key:            HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:            HKLM\system\currentcontrolset\control\srp\gp\dll
  Opens key:            HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:            HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:            HKCU\
  Opens key:            HKCU\control panel\desktop\muicached\machinelanguageconfiguration
  Opens key:            HKLM\software\policies\microsoft\mui\settings
  Opens key:            HKCU\software\policies\microsoft\control panel\desktop
  Opens key:            HKCU\control panel\desktop\languageconfiguration
  Opens key:            HKCU\control panel\desktop
  Opens key:            HKCU\control panel\desktop\muicached
  Opens key:            HKLM\software\microsoft\windows\currentversion\sidebyside
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:            HKLM\system\currentcontrolset\control\nls\sorting\versions
  Opens key:            HKLM\system\currentcontrolset\control\error message instrument\
  Opens key:            HKLM\system\currentcontrolset\control\error message instrument
  Opens key:            HKLM\software\microsoft\windows nt\currentversion\gre_initialize
  Opens key:            HKLM\software\microsoft\windows nt\currentversion\compatibility32
  Opens key:            HKLM\software\microsoft\windows nt\currentversion\ime compatibility
  Opens key:            HKLM\
  Opens key:            HKLM\software\microsoft\windows nt\currentversion\windows
  Opens key:            HKLM\software\microsoft\windows nt\currentversion\diagnostics
  Opens key:            HKLM\software\microsoft\ole
  Opens key:            HKLM\software\microsoft\ole\tracing
  Opens key:            HKLM\software\microsoft\windows\currentversion\policies\explorer
  Opens key:            HKCU\software\microsoft\windows\currentversion\policies\explorer
  Opens key:            HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:            HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\afdd75bce006a193064e6227738b4bea.exe
  Opens key:            HKLM\software\microsoft\oleaut
  Opens key:            HKCU\software\classes\
  Opens key:            HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder
  Opens key:            HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder
  Opens key:            HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}\shellfolder
  Opens key:            HKLM\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}\shellfolder
  Opens key:            HKCU\software\microsoft\windows\currentversion\policies\nonenum
  Opens key:            HKLM\software\microsoft\windows\currentversion\policies\nonenum
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{69d250e4-6c18-
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:
HKLM\software\microsoft\windows\shell\registeredapplications\urlassociations\directory\openwithprogids
Opens key:
HKCU\software\microsoft\windows\shell\associations\urlassociations\directory
Opens key:                    HKCU\software\classes\directory
Opens key:                    HKCR\directory
Opens key:                    HKCU\software\classes\directory\curver
Opens key:                    HKCR\directory\curver
Opens key:                    HKCR\directory\
Opens key:                    HKCU\software\classes\directory\shellex\iconhandler
Opens key:                    HKCR\directory\shellex\iconhandler
Opens key:                    HKCU\software\classes\folder
Opens key:                    HKCR\folder
Opens key:                    HKCU\software\classes\folder\shellex\iconhandler
Opens key:                    HKCR\folder\shellex\iconhandler
Opens key:                    HKCU\software\classes\allfilesystemobjects
Opens key:                    HKCR\allfilesystemobjects
Opens key:                    HKCU\software\classes\allfilesystemobjects\shellex\iconhandler
Opens key:                    HKCR\allfilesystemobjects\shellex\iconhandler
Opens key:                    HKCU\software\classes\directory\docobject
Opens key:                    HKCR\directory\docobject
Opens key:                    HKCU\software\classes\folder\docobject
Opens key:                    HKCR\folder\docobject
Opens key:                    HKCU\software\classes\allfilesystemobjects\docobject
Opens key:                    HKCR\allfilesystemobjects\docobject
Opens key:                    HKCU\software\classes\directory\browseinplace
Opens key:                    HKCR\directory\browseinplace
Opens key:                    HKCU\software\classes\folder\browseinplace
Opens key:                    HKCR\folder\browseinplace
Opens key:                    HKCU\software\classes\allfilesystemobjects\browseinplace
Opens key:                    HKCR\allfilesystemobjects\browseinplace
Opens key:                    HKCU\software\classes\directory\clsid
Opens key:                    HKCR\directory\clsid
Opens key:                    HKCU\software\classes\folder\clsid
Opens key:                    HKCR\folder\clsid
Opens key:                    HKCU\software\classes\allfilesystemobjects\clsid
Opens key:                    HKCR\allfilesystemobjects\clsid
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}\propertybag
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:                    HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid
Opens key:                    HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32
Opens key:                    HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32
Opens key:                    HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler32
Opens key:                    HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler32
Opens key:                    HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler
Opens key:                    HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler
Opens key:                    HKLM\system\currentcontrolset\control\lsa\accessproviders
Opens key:                    HKLM\system\currentcontrolset\services\ldap
```

```
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings
   Opens key:                 HKLM\system\currentcontrolset\control\cmf\config
   Opens key:                 HKLM\software\microsoft\windows\windows error reporting\wmr
   Opens key:                 HKLM\software\microsoft\windows\currentversion\setup
   Opens key:                 HKLM\software\microsoft\windows\currentversion
   Opens key:                 HKLM\software\microsoft\rpc
   Opens key:                 HKLM\system\currentcontrolset\control\computername\activecomputername
   Opens key:                 HKLM\system\setup
   Opens key:                 HKLM\software\policies\microsoft\windows nt\rpc
   Opens key:                 HKLM\software\policies\microsoft\sqmclient\windows
   Opens key:                 HKLM\software\microsoft\sqmclient\windows
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-
b4ef-bd1dc332aeae}
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-
b4ef-bd1dc332aeae}\propertybag
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}\propertybag
   Opens key:
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:                 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:             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[afdd75bce006a193064e6227738b4bea]
   Queries value:             HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
   Queries value:             HKLM\software\microsoft\ole[pageallocatorusesystemheap]
   Queries value:             HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
   Queries value:             HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
   Queries value:             HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
   Queries value:            HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
   Queries value:            HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[callforattributes]
   Queries value:            HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[restrictedattributes]
   Queries value:            HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsfordisplay]
   Queries value:            HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hidefolderverbs]
   Queries value:            HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[usedrophandler]
   Queries value:            HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsforparsing]
   Queries value:            HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsparsedisplayname]
   Queries value:            HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforoverlay]
   Queries value:            HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[mapnetdriveverbs]
   Queries value:            HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
```

08002b30309d}\shellfolder[queryforinfotip]
   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]
   Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[pintonamespacetree]
   Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hasnavigationenum]
   Queries 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]
   Queries value: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
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]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
   Queries 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]
   Queries 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:
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: HKCR\directory[alwaysshowext]
   Queries value: HKCR\directory[nevershowext]
   Queries value: HKCR\folder[nevershowext]
   Queries value: HKCR\allfilesystemobjects[nevershowext]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[category]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[name]

```
    Queries 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-424c-
b029-7fe99a87c641}[description]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[relativepath]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[parsingname]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[infotip]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[localizedname]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[icon]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[security]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[streamresource]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[streamresourcetype]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[localredirectonly]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[roamable]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[precreate]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[stream]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[publishexpandedpath]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[attributes]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[foldertypeid]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[initfolderhandler]
    Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[desktop]
    Queries value:              HKLM\software\microsoft\com3[com+enabled]
    Queries value:              HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
    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\system\currentcontrolset\control\cmf\config[system]
    Queries value:              HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
    Queries value:              HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
    Queries value:              HKLM\software\microsoft\windows\currentversion[devicepath]
    Queries value:              HKLM\software\microsoft\rpc[maxrpcsize]
```

Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
 Queries value: HKLM\system\setup[oobeinprogress]
 Queries value: HKLM\system\setup[systemsetupinprogress]
 Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[category]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[name]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[parentfolder]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[description]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[relativepath]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[parsingname]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[infotip]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[localizedname]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[icon]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[security]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[streamresource]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[streamresourcetype]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[localredirectonly]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[roamable]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[precreate]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[stream]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[publishexpandedpath]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[attributes]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[foldertypeid]
 Queries 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}]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[category]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[name]
 Queries value:

```
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:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[relativepath]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[parsingname]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[infotip]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[localizedname]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[icon]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[security]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[streamresource]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[streamresourcetype]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[localredirectonly]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[roamable]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[precreate]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[stream]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[publishexpandedpath]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[attributes]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[foldertypeid]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[initfolderhandler]
    Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[category]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[name]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[parentfolder]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[description]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[relativepath]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[parsingname]
    Queries value:
```

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[infotip]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localizedname]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[icon]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{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]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localredirectonly]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[roamable]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[precreate]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[stream]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[foldertypeid]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler]
   Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-2160590473-689474908-1361669368-1002[profileimagepath]
   Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll]