Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	270
Risk Level:	1
Date Processed:	2016-04-28 12:54:18 (UTC)
Processing Time:	61.11 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\1edab3297a51c34ae2782d399a89b328.exe"

Sample ID:	68
Type:	basic
Owner:	admin
Label:	1edab3297a51c34ae2782d399a89b328
Date Added:	2016-04-28 12:44:56 (UTC)
File Type:	PE32:win32:gui
File Size:	360448 bytes
MD5:	1edab3297a51c34ae2782d399a89b328
SHA256:	86ab6c7b128b020d5a9a6fc179576b65f1b021b7e915ce512be2fb24393d70dc
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process:	C:\windows\temp\1edab3297a51c34ae2782d399a89b328.exe ["C:\windows\temp\1edab3297a51c34ae2782d399a89b328.exe"]

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates semaphore:	\Sessions\1\BaseNamedObjects\C:?WINDOWS?TEMP?1EDAB3297A51C34AE2782D399A89B328.EXE

File System Events

Opens:	C:\Windows\Prefetch\1EDAB3297A51C34AE2782D399A89B-849703DA.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\1edab3297a51c34ae2782d399a89b328.exe
Opens:	C:\Windows\SysWOW64\ntdll.dll
Opens:	C:\Windows\SysWOW64\kernel32.dll
Opens:	C:\Windows\SysWOW64\KernelBase.dll
Opens:	C:\Windows\apppatch\sysmain.sdb
Opens:	C:\Windows\SysWOW64\msvbvm60.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\combase.dll
Opens:	C:\Windows\SysWOW64\gdi32.dll
Opens:	C:\Windows\SysWOW64\user32.dll
Opens:	C:\Windows\SysWOW64\msvcrt.dll
Opens:	C:\Windows\SysWOW64\bcryptprimitives.dll
Opens:	C:\Windows\SysWOW64\cryptbase.dll
Opens:	C:\Windows\SysWOW64\sspicli.dll
Opens:	C:\Windows\SysWOW64\rpcrt4.dll
Opens:	C:\Windows\SysWOW64\advapi32.dll
Opens:	C:\Windows\SysWOW64\ole32.dll
Opens:	C:\Windows\SysWOW64\oleaut32.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\SysWOW64\msctf.dll
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\Windows\SysWOW64\uxtheme.dll
Opens:	C:\Windows\SysWOW64\sxs.dll
Opens:	C:\Windows\SysWOW64\clbcatq.dll
Opens:	C:\Windows\SysWOW64\shlwapi.dll
Opens:	C:\Windows\SysWOW64\shell32.dll
Opens:	C:\Windows\SysWOW64\SHCore.dll
Opens:	C:\
Opens:	C:\Windows\SysWOW64\propsys.dll
Opens:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000000e.db
Opens:	C:\Program Files (x86)\desktop.ini
Opens:	C:\Windows\SysWOW64\cfgmgr32.dll
Opens:	C:\Windows\SysWOW64\devobj.dll
Opens:	C:\Windows\SysWOW64\setupapi.dll
Opens:	C:\Windows\SysWOW64\scrrun.dll
Opens:	C:\Windows\SysWOW64\version.dll
Opens:	C:\Windows\Temp

```
  Opens:                    C:\windows\temp\audomate4.ini
  Opens:                    C:\Windows\Fonts\StaticCache.dat
  Opens:                    C:\Windows\SysWOW64\dwmapi.dll
  Opens:                    C:\Windows\Fonts\sserife.fon
  Reads from:               C:\Program Files (x86)\desktop.ini
  Reads from:               C:\Windows\SysWOW64\scrrun.dll
  Reads from:               C:\Windows\Fonts\StaticCache.dat
```

Windows Registry Events

```
  Opens key:                HKLM\software\microsoft\wow64
  Opens key:                HKLM\system\currentcontrolset\control\terminal server
  Opens key:                HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:                HKLM\system\currentcontrolset\control\srp\gp\dll
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:                HKLM\system\currentcontrolset\control\nls\language
  Opens key:                HKLM\system\currentcontrolset\control\mui\uilanguages
  Opens key:                HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
  Opens key:                HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
  Opens key:                HKLM\software\wow6432node\policies\microsoft\mui\settings
  Opens key:                HKLM\software\policies\microsoft\mui\settings
  Opens key:                HKCU\
  Opens key:                HKCU\control panel\desktop\muicached\machinelanguageconfiguration
  Opens key:                HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
  Opens key:                HKCU\software\policies\microsoft\control panel\desktop
  Opens key:                HKCU\control panel\desktop\languageconfiguration
  Opens key:                HKCU\control panel\desktop
  Opens key:                HKCU\control panel\desktop\muicached
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
  Opens key:                HKLM\system\currentcontrolset\control\nls\sorting\versions
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
  Opens key:                HKCU\software\microsoft\windows nt\currentversion\appcompatflags
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation
  Opens key:                HKLM\system\currentcontrolset\control\session manager
  Opens key:                HKLM\software\wow6432node\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\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
  Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32
  Opens key:                HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
  Opens key:                HKLM\
  Opens key:                HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
  Opens key:                HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
  Opens key:                HKLM\system\currentcontrolset\control\lsa
  Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
  Opens key:                HKLM\software\wow6432node\microsoft\ole
  Opens key:                HKLM\software\wow6432node\microsoft\ole\tracing
  Opens key:                HKLM\software\microsoft\ole\tracing
  Opens key:                HKLM\software\wow6432node\microsoft\oleaut
  Opens key:                HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:                HKLM\system\currentcontrolset\control\nls\sorting\ids
  Opens key:                HKLM\system\currentcontrolset\control\nls\locale
  Opens key:                HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
  Opens key:                HKLM\system\currentcontrolset\control\nls\language groups
  Opens key:                HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
  Opens key:                HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:                HKLM\software\microsoft\sqmclient\windows
  Opens key:                HKCU\software\microsoft\windows\currentversion\directmanipulation
  Opens key:                HKLM\system\currentcontrolset\control\nls\codepage
  Opens key:                HKLM\software\wow6432node\microsoft\vba\monitors
  Opens key:                HKCU\software\classes\
  Opens key:                HKLM\software\microsoft\com3
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{2e2c5836-6406-4e06-99a7-
e8e8cae58e8b}
  Opens key:                HKCR\activatableclasses\clsid
  Opens key:                HKCR\activatableclasses\clsid\{2e2c5836-6406-4e06-99a7-e8e8cae58e8b}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{2e2c5836-6406-4e06-99a7-
e8e8cae58e8b}
  Opens key:                HKCR\wow6432node\clsid\{2e2c5836-6406-4e06-99a7-e8e8cae58e8b}
  Opens key:                HKCU\software\classes\clsid\{2e2c5836-6406-4e06-99a7-e8e8cae58e8b}
  Opens key:                HKCR\clsid\{2e2c5836-6406-4e06-99a7-e8e8cae58e8b}
  Opens key:                 HKCU\software\classes\activatableclasses\clsid
  Opens key:                 HKCU\software\classes\activatableclasses\clsid\{2e2c5836-6406-4e06-99a7-
e8e8cae58e8b}
  Opens key:                 HKLM\software\wow6432node\diepol\audomate4\
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}\propertybag
  Opens key:                 HKLM\software\wow6432node\microsoft\windows\currentversion
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}\propertybag
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer
  Opens key:                 HKLM\software\microsoft\windows\currentversion\policies\explorer
  Opens key:                 HKCU\software\microsoft\windows\currentversion\policies\explorer
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\1edab3297a51c34ae2782d399a89b328.exe
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder
  Opens key:                 HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}\shellfolder
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-
a2d8-08002b30309d}\shellfolder
  Opens key:                 HKCU\software\microsoft\windows\currentversion\policies\nonenum
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\nonenum
  Opens key:                 HKLM\software\microsoft\windows\currentversion\policies\nonenum
  Opens key:                 HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-
11e3-be65-806e6f6e6963}\
  Opens key:                 HKCU\software\classes\drive\shellex\folderextensions
  Opens key:                 HKCR\drive\shellex\folderextensions
  Opens key:                 HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-
4442-804e-409d6c4515e9}
  Opens key:                 HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}
  Opens key:                 HKLM\software\wow6432node\policies\microsoft\windows\explorer
  Opens key:                 HKLM\software\policies\microsoft\windows\explorer
  Opens key:                 HKCU\software\policies\microsoft\windows\explorer
  Opens key:                 HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-
a6bb2164fbd0}\inprocserver32
  Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}
  Opens key:                 HKCR\activatableclasses\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}
  Opens key:                 HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\treatas
  Opens key:                 HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32
  Opens key:                 HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler32
  Opens key:                 HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler
  Opens key:                 HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler
  Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}
```

```
  Opens key:              HKCR\activatableclasses\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}
  Opens key:              HKCU\software\classes\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}
  Opens key:              HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}
  Opens key:              HKCU\software\classes\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\treatas
  Opens key:              HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\treatas
  Opens key:              HKCU\software\classes\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\inprocserver32
  Opens key:              HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\inprocserver32
  Opens key:              HKCU\software\classes\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\inprochandler32
  Opens key:              HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\inprochandler32
  Opens key:              HKCU\software\classes\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\inprochandler
  Opens key:              HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\inprochandler
  Opens key:              HKLM\software\wow6432node\microsoft\windows\currentversion\setup
  Opens key:              HKLM\software\microsoft\windows\currentversion\setup
  Opens key:              HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}
  Opens key:              HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\properties
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-
11e3-be65-806e6f6e6963}\
  Opens key:              HKCU\software\classes\typelib
  Opens key:              HKCR\typelib
  Opens key:              HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-00a0c9054228}
  Opens key:              HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}
  Opens key:              HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0
  Opens key:              HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0
  Opens key:              HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-
00a0c9054228}\1.0\0
  Opens key:              HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0
  Opens key:              HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-
00a0c9054228}\1.0\0\win32
  Opens key:              HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0\win32
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
  Opens key:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\segoe ui
  Opens key:
HKLM\software\wow6432node\microsoft\ctf\compatibility\1edab3297a51c34ae2782d399a89b328.exe
  Opens key:              HKLM\software\wow6432node\microsoft\ctf\
  Queries value:          HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:          HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[empty]
  Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
  Queries value:          HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
  Queries value:          HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
  Queries value:          HKCU\control panel\desktop[preferreduilanguages]
  Queries value:          HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Queries value:          HKLM\system\currentcontrolset\control\nls\sorting\versions[]
  Queries value:          HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
  Queries value:          HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  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[msvbvm60.dll]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[1edab3297a51c34ae2782d399a89b328.exe]
  Queries value:          HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:          HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[1edab3297a51c34ae2782d399a89b328]
  Queries value:          HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:          HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
```

```
   Queries value:              HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
   Queries value:              HKLM\software\microsoft\ole[pageallocatorusesystemheap]
   Queries value:              HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
   Queries value:              HKLM\software\microsoft\ole[aggressivemtatesting]
   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\control\nls\sorting\versions[000602xx]
   Queries value:              HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
   Queries value:              HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000409]
   Queries value:              HKLM\system\currentcontrolset\control\nls\language groups[1]
   Queries value:              HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
   Queries value:              HKLM\software\microsoft\sqmclient\windows[ceipenable]
   Queries value:              HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
   Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[932]
   Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[949]
   Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[950]
   Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[936]
   Queries value:              HKLM\software\microsoft\com3[com+enabled]
   Queries value:              HKLM\software\microsoft\ole[maxsxshashcount]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[category]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[name]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[parentfolder]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[description]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[relativepath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[parsingname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[infotip]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[localizedname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[icon]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[security]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[streamresource]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[streamresourcetype]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[localredirectonly]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[roamable]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[precreate]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[stream]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[publishexpandedpath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[attributes]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[foldertypeid]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[initfolderhandler]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[category]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[name]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[parentfolder]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[description]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[relativepath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[parsingname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[infotip]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[localizedname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[icon]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[security]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresource]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresourcetype]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[localredirectonly]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[roamable]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[precreate]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[stream]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[publishexpandedpath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[attributes]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[foldertypeid]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[initfolderhandler]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
   Queries value:              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
   Queries value:              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[callforattributes]
   Queries value:              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[restrictedattributes]
```

```
   Queries value:              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[foldervalueflags]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}]
   Queries value:              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32[]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-
11e3-be65-806e6f6e6963}[data]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-
11e3-be65-806e6f6e6963}[generation]
   Queries value:              HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
   Queries value:              HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-
a6bb2164fbd0}\inprocserver32[]
   Queries value:              HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
   Queries value:              HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[inprocserver32]
   Queries value:              HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[]
   Queries value:              HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[threadingmodel]
   Queries value:              HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}[]
   Queries value:              HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\inprocserver32[inprocserver32]
   Queries value:              HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\inprocserver32[]
   Queries value:              HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\inprocserver32[threadingmodel]
   Queries value:              HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
   Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-
11e3-be65-806e6f6e6963}[data]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-
11e3-be65-806e6f6e6963}[generation]
   Queries value:              HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0\win32[]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
   Queries value:              HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
```