Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 68, Task ID: 270

Task ID: 270

Risk Level:

Date Processed: 2016-04-28 12:54:18 (UTC)

Processing Time: 61.11 seconds Virtual Environment: IntelliVM

"c:\windows\temp\1edab3297a51c34ae2782d399a89b328.exe" **Execution Arguments:**

Sample ID: Type: basic Owner: admin

Label: 1edab3297a51c34ae2782d399a89b328

Date Added: 2016-04-28 12:44:56 (UTC)

File Type: PE32:win32:gui File Size: 360448 bytes

1edab3297a51c34ae2782d399a89b328 MD5:

SHA256: 86ab6c7b128b020d5a9a6fc179576b65f1b021b7e915ce512be2fb24393d70dc

Description:

Pattern Matching Results

Process/Thread Events

C:\windows\temp\1edab3297a51c34ae2782d399a89b328.exe Creates process:

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

Named Object Events

\Sessions\1\BaseNamedObjects\DBWinMutex Creates mutex: 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

C:\Windows\SysWOW64\ntdll.dll Opens: C:\Windows\SysWOW64\kernel32.dll Opens: Opens: C:\Windows\SysWOW64\KernelBase.dll Opens: C:\Windows\apppatch\sysmain.sdb Opens: C:\Windows\SysWOW64\msvbvm60.dll C:\Windows\SysWOW64\sechost.dll Opens: Opens: C:\Windows\SysWOW64\combase.dll C:\Windows\SysWOW64\gdi32.dll Opens: Opens: C:\Windows\SysWOW64\user32.dll C:\Windows\SysWOW64\msvcrt.dll Opens:

Opens: C:\Windows\SysWOW64\bcryptprimitives.dll

Opens: C:\Windows\SysWOW64\cryptbase.dll C:\Windows\SysWOW64\sspicli.dll Opens: C:\Windows\SysWOW64\rpcrt4.dll Opens: C:\Windows\SysWOW64\advapi32.dll Opens: Opens: C:\Windows\SysWOW64\ole32.dll C:\Windows\SysWOW64\oleaut32.dll Opens: 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 C:\Windows\SysWOW64\sxs.dll Opens: Opens: C:\Windows\SysWOW64\clbcatq.dll Opens: C:\Windows\SysWOW64\shlwapi.dll C:\Windows\SysWOW64\shell32.dll Opens: C:\Windows\SysWOW64\SHCore.dll Opens: C:\ Opens:

Opens: C:\Windows\SysWOW64\propsys.dll

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

4C77-AF34-C647E37CA0D9}.1.ver0x000000000000000e.db

Opens: C:\Program Files (x86)\desktop.ini C:\Windows\SysWOW64\cfgmgr32.dll Opens: Opens: C:\Windows\SysWOW64\devobj.dll C:\Windows\SysWOW64\setupapi.dll Opens: 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\currentcontrol\set\control\terminal server
Opens key: HKLM\system\currentcontrol\set\control\safeboot\option
Opens key: HKLM\system\currentcontrol\set\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\currentcontrol\set\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\currentcontrol\st\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

 $Opens~key: \\ \qquad \qquad HKLM\system\current control\set\control\slasorithm policy$

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\currentcontrol\nls\extendedlocale
Opens key: HKLM\system\currentcontrol\st\control\nls\sorting\ids
Opens key: HKLM\system\currentcontrol\set\control\nls\locale

 $Opens~key: \\ HKLM\system\currentcontrolset\control\nls\locale\alternate~sorts$

Opens key: ${\tt HKLM \backslash system \backslash current control \backslash nls \backslash language \ groups}$

 $Opens\ key: \\ HKLM\software\wow6432 node\microsoft\windows\windows\ error\ reporting\wmr$

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\www6432node\clsid\{2e2c5836-6406-4e06-99a7-e8e8cae58e8b}

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 kev: HKCU\software\classes\activatableclasses\clsid\{2e2c5836-6406-4e06-99a7-

e8e8cae58e8b}

Opens key: HKLM\software\wow6432node\diepol\audomate4\

Opens key:

Opens key:

c1bf-494e-b29c-65b732d3d21a}

Opens key:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{905e63b6-1008\} \\ folder \\ folder \\ descr$

c1bf-494e-b29c-65b732d3d21a}\propertybag

HKLM\software\wow6432node\microsoft\windows\currentversion

Opens key:

a0fb-4bfc-874a-c0f2e0b9fa8e}

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-microsoft \ windows \ explorer \ folder \ descriptions \ explorer \ folder \$

 $a Ofb-4bfc-874a-c Of 2e Ob 9fa 8e \} \\ \label{eq:condition}$

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:

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

08002b30309d}\shellfolder

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

08002b30309d}\shellfolder

Opens key:

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

Opens key:

a2d8-08002b30309d}\shellfolder

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

Opens key:

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum \setminus microsoft \setminus windows \setminus current version \setminus microsoft \setminus windows \setminus current version \setminus microsoft \setminus$

Opens kev: 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:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c64-7c88-4c64-7c$

11e3-be65-806e6f6e6963}\

Opens key: HKCU\software\classes\drive\shellex\folderextensions

Opens key: HKCR\drive\shellex\folderextensions

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \drive\shellex \folder extensions \fine \classes \drive\shellex \folder \end{tabular} \end{tabular}$ Opens key:

4442-804e-409d6c4515e9}

HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-

409d6c4515e9}

Opens key:

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 HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-Opens key:

a6bb2164fbd0}\inprocserver32

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}

HKCR\activatableclasses\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}

Opens key:

HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\treatas

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprocserver32

 $HKCU \setminus software \setminus classes \setminus wow 6432 node \setminus clsid \setminus \{1f486a52 - 3cb1 - 48fd - 8f50 -$ Opens key:

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler

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

b8dc300d9f9d}\inprochandler

Opens key:

00a0c9054228}

Opens key: HKCR\activatableclasses\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228} Opens key: HKCU\software\classes\ww6432node\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}

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\currentcontrol\set\control\deviceclasses\{53f5630d-b6bf-11d0-

94f2-00a0c91efb8b}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-

94f2-00a0c91efb8b}\properties

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c63-7c88-4c41, d124, d244, d$

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

 $\verb|nt\currentversion\language| pack\surrogatefall back|$

Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\segoe ui

Opens key:

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:

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:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [prefer external manifest]] \ details a side by side \ details a side \ details a side by side \ details a side$

Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]

Queries value: HKCU\software\microsoft\windows

 $\verb|nt\currentversion\appcompatflags[showdebuginfo]|\\$

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

 $\verb|nt\currentversion\windows[loadappinit_dlls]| \\$

Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]

```
HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Oueries value:
Oueries 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]
Oueries value:
                        HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
Queries value:
                        HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
Oueries 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]
```

reporting\wmr[disable]

Oueries value:

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:

 $\label{thm:local-bound} $HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a\}[category]$}$

HKLM\software\wow6432node\microsoft\windows\windows error

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} [name]$

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} [description]$

Queries value:

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \cdot \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} [infotip]$

Queries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} \ [localized name]$

Queries value:

 $\label{thm:local-ham} $$HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a\}[icon]}$

Queries value:

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

Queries value:

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

Oueries value

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \cite{200} folder \cite{200} fol$

Queries value:

 $\label{localized-optimiz$

Queries value:

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

Queries value:

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

Oueries value

 $\label{local-HKLM} HKLM software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \cite{200} and \cite{20$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma\{905e63b6-c1bf-494e-b29c-65b732d3d21a\}[publishexpandedpath]$

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} [folder typeid]$

Oueries value

 $\label{thm:local_ham} \begin{tabular}{ll} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdescripti$

c1bf-494e-b29c-65b732d3d21a}[initfolderhandler] Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir] Queries value: a0fb-4bfc-874a-c0f2e0b9fa8e}[category] Oueries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-microsoft \ windows \ explorer \ folder \ description \ explorer \ folder \$ a0fb-4bfc-874a-c0f2e0b9fa8e}[name] Queries value: $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus windows \setminus current \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus windows \setminus windows \setminus windows \setminus windows \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus windows \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \\ descriptions \setminus wi$ a0fb-4bfc-874a-c0f2e0b9fa8e}[parentfolder] a0fb-4bfc-874a-c0f2e0b9fa8e}[description] Oueries value: a0fb-4bfc-874a-c0f2e0b9fa8e}[relativepath] Oueries value: a0fb-4bfc-874a-c0f2e0b9fa8e}[parsingname] Queries value: a0fb-4bfc-874a-c0f2e0b9fa8e}[infotip] Oueries value: a0fb-4bfc-874a-c0f2e0b9fa8e}[localizedname] Oueries value: a0fb-4bfc-874a-c0f2e0b9fa8e}[icon] Oueries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-microsoft \ windows \ explorer \ folder \ description \ explorer \ folder \$ a0fb-4bfc-874a-c0f2e0b9fa8e}[security] Oueries value: $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus windows \setminus current \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus windows \setminus windows \setminus windows \setminus windows \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus windows \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \\ descriptions \setminus wi$ a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresource] Queries value: a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresourcetype] Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40efa0fb-4bfc-874a-c0f2e0b9fa8e}[localredirectonly] Oueries value: $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus windows \setminus current \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus windows \setminus windows \setminus windows \setminus windows \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus windows \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \\ descriptions \setminus wi$ a0fb-4bfc-874a-c0f2e0b9fa8e}[roamable] Queries value: a0fb-4bfc-874a-c0f2e0b9fa8e}[precreate] Oueries value: a0fb-4bfc-874a-c0f2e0b9fa8e}[stream] Oueries value: a0fb-4bfc-874a-c0f2e0b9fa8e}[publishexpandedpath] Oueries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-microsoft \ windows \ explorer \ folder \ description \ explorer \ folder \$ a0fb-4bfc-874a-c0f2e0b9fa8e}[attributes] Oueries value: $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus windows \setminus current \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus windows \setminus windows \setminus windows \setminus windows \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus windows \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \\ descriptions \setminus wi$ a0fb-4bfc-874a-c0f2e0b9fa8e}[foldertypeid] a0fb-4bfc-874a-c0f2e0b9fa8e}[initfolderhandler] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer] Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin] HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel] HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon] Oueries value:

HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\shellfolder[attributes] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Queries value: 08002b30309d}\shellfolder[callforattributes] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[restrictedattributes]

```
Oueries 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]
    Oueries value:
11e3-be65-806e6f6e6963}[generation]
                                                                HKCR \ drive \ bellex \ folder extensions \ \{fbeb8a05-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4442-804e-beee-4446-beee-4446-beee-4446-beee-4446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-beee-466-
    Queries value:
409d6c4515e9}[drivemask]
                                                                HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-
    Oueries value:
a6bb2164fbd0}\inprocserver32[]
                                                                HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
    Queries value:
    Oueries value:
                                                                HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[inprocserver32]
                                                                HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
    Oueries value:
b8dc300d9f9d}\inprocserver32[]
                                                                HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
    Queries value:
b8dc300d9f9d}\inprocserver32[threadingmodel]
                                                                HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}[]
    Queries value:
                                                                HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
    Oueries value:
00a0c9054228}\inprocserver32[inprocserver32]
                                                                HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
    Oueries value:
00a0c9054228}\inprocserver32[]
                                                                HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
    Queries value:
00a0c9054228}\inprocserver32[threadingmodel]
    Queries value:
                                                                HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
    Oueries value:
                                                                HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
    Queries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mountpoints 2 \setminus cpc \setminus volume \setminus \{d5291c63-7c88-five a property of the pr
11e3-be65-806e6f6e6963}[data]
    Queries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c63-7c88-4c64, d5291c63-7c88-4c64, d5291c64, d5291c64, d5291c64, d5291c64, d5291c64, d5291c64, d5291c64, d5291c644, d5291c64, d5291c64, d5291c64, d5291c64, d5291c64, d5291c64, 
11e3-be65-806e6f6e6963}[generation]
                                                                HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0\win32[]
    Oueries value:
    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]
    Oueries value:
                                                                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
                                                                HKLM\software\microsoft\windows
    Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane2]|
                                                                HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\languagepack\surrogatefallback[plane3]
                                                                HKLM\software\microsoft\windows
    Queries value:
\verb|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]
                                                                HKLM\software\microsoft\windows
    Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane7]
                                                                HKLM\software\microsoft\windows
    Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane8]
    Queries value:
                                                                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
                                                                HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\languagepack\surrogatefallback[plane10]
    Queries value:
                                                                HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback[plane11]|
    Queries value:
                                                                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
                                                                HKLM\software\microsoft\windows
    Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane13]
                                                                HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\languagepack\surrogatefallback[plane14]
                                                                HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\languagepack\surrogatefallback[plane15]
                                                                HKLM\software\microsoft\windows
```

HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]

 $\verb|nt\currentversion\languagepack\surrogatefallback[plane16]|$

Queries value: