Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 37, Task ID: 148

Task ID: 148

Risk Level:

Date Processed: 2016-04-28 12:50:53 (UTC)

Processing Time: 62.73 seconds Virtual Environment: IntelliVM

"c:\windows\temp\7842072cea4eb57a03bdd00b54088404.exe" **Execution Arguments:**

Sample ID: Type: basic Owner: admin

Label: 7842072cea4eb57a03bdd00b54088404

Date Added: 2016-04-28 12:44:53 (UTC)

File Type: PE32:win32:gui File Size: 807276 bytes

7842072cea4eb57a03bdd00b54088404 MD5:

SHA256: c1fe42986e89fd92ef404ed5ef57f650abb3eb526f77f3fb30a1167b1ab1791b

Description:

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

C:\windows\temp\7842072cea4eb57a03bdd00b54088404.exe

["C:\windows\temp\7842072cea4eb57a03bdd00b54088404.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0

Creates mutex:

Creates event: \KernelObjects\MaximumCommitCondition

Creates event: \Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1

File System Events

C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches Creates:

Creates: C:\Users\Admin\AppData\Local\Temp\

C:\Users\Admin\AppData\Local\Temp\nso5232.tmp Creates: Creates: C:\Users\Admin\AppData\Local\Temp\nsz53AA.tmp

Creates: C:\Program Files (x86)

Creates: C:\Users\Admin\AppData\Local\Temp\nso53BA.tmp

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

Creates: C:\Users\Admin\AppData Creates: C:\Users\Admin\AppData\Local Creates: C:\Users\Admin\AppData\Local\Temp

C:\Users\Admin\AppData\Local\Temp\nso53BA.tmp\test.ini Creates: C:\Windows\Prefetch\7842072CEA4EB57A03BDD00B54088-6F31F437.pf Opens:

Opens: C:\Windows

C:\Windows\System32\wow64.dll Opens: Opens: C:\Windows\System32\wow64win.dll Opens: C:\Windows\System32\wow64cpu.dll C:\Windows\system32\wow64log.dll Opens:

Opens: C:\Windows\SysWOW64

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

Opens: C:\windows\temp\7842072cea4eb57a03bdd00b54088404.exe.Local\

Opens: C:\Windows\winsxs\x86_microsoft.windows.common-

controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2

Opens: C:\Windows\winsxs\x86_microsoft.windows.commoncontrols_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll

Opens: C:\windows\temp\VERSION.dll C:\Windows\SysWOW64\version.dll Opens: Opens: C:\Windows\SysWOW64\apphelp.dll Opens: C:\Windows\AppPatch\sysmain.sdb

 $C: \verb|\windows| Temp| 7842072 cea 4eb 57a 03bdd 00b 54088404.exe|$ Opens:

Opens: C:\Windows\AppPatch\AcGenral.dll Opens: C:\windows\temp\UxTheme.dll Opens: C:\Windows\SysWOW64\uxtheme.dll Opens: C:\windows\temp\WINMM.dll

C:\Windows\SysWOW64\winmm.dll Opens: Opens: C:\windows\temp\samcli.dll Opens: C:\Windows\SysWOW64\samcli.dll Opens: C:\windows\temp\MSACM32.dll C:\Windows\SysWOW64\msacm32.dll Opens: Opens: C:\windows\temp\sfc.dll Opens: C:\Windows\SysWOW64\sfc.dll Opens: C:\windows\temp\sfc_os.DLL Opens: C:\Windows\SysWOW64\sfc_os.dll Opens: C:\windows\temp\USERENV.dll Opens: C:\Windows\SysWOW64\userenv.dll C:\windows\temp\profapi.dll Opens: Opens: C:\Windows\SysWOW64\profapi.dll Opens: C:\windows\temp\dwmapi.dll Opens: C:\Windows\SysWOW64\dwmapi.dll Opens: C:\windows\temp\MPR.dll Opens: C:\Windows\SysWOW64\mpr.dll Opens: C:\Windows\SysWOW64\imm32.dll Opens:

C:\windows\temp\7842072cea4eb57a03bdd00b54088404.exe.Config

Opens: C:\Windows\WindowsShell.Manifest Opens:

C:\Windows\SysWOW64\en-US\setupapi.dll.mui

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

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

Opens: C:\Windows\SysWOW64\shell32.dll

Opens:

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

Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db

Opens: C:\windows\temp\ntmarta.dll Opens: C:\Windows\SysWOW64\ntmarta.dll

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

4C77-AF34-C647E37CA0D9}.1.ver0x000000000000001.db

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

C:\Users\Admin\AppData\Local\Temp\nso5232.tmp Opens:

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

Opens: C:\Users\Admin\AppData Opens: C:\Users\Admin\AppData\Local Opens: C:\Program Files (x86)

Opens: C:\Program Files (x86)\desktop.ini

Opens: ${\tt C:\Users\Admin\AppData\Local\Temp\nso53BA.tmp}$

Opens: C:\Users\Admin\AppData\Local\Temp\nso53BA.tmp\test.ini

Opens: C:\windows\temp\RichEd20.dll Opens: C:\Windows\SysWOW64\riched20.dll Opens: C:\Windows\Fonts\tahoma.ttf

C:\Windows\SysWOW64\en-US\user32.dll.mui Opens:

Opens: C:\Windows\SysWOW64\ole32.dll

Opens: C:\Windows\win.ini

Opens: C:\Windows\SysWOW64\UxTheme.dll.Config

Opens: C:\Windows\Fonts\StaticCache.dat

Writes to: C:\Users\Admin\AppData\Local\Temp\nsz53AA.tmp

Writes to: C:\Users\Admin\AppData\Local\Temp\nso53BA.tmp\test.ini

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

C:\Windows\Temp\7842072cea4eb57a03bdd00b54088404.exe Reads from: Reads from: $C: \verb|\Users\Admin\AppData\Local\Temp\nsz53AA.tmp| \\$

Reads from: C:\Program Files (x86)\desktop.ini

C:\Windows\win.ini Reads from:

Reads from: C:\Windows\Fonts\StaticCache.dat

Deletes: C:\Users\Admin\AppData\Local\Temp\nso5232.tmp Deletes: C:\Users\Admin\AppData\Local\Temp\nso53BA.tmp

Windows Registry Events

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

options

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

Opens key: HKLM\software\microsoft\wow64

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file

execution options

Opens kev: HKLM\system\currentcontrolset\control\terminal server Opens key: ${\tt HKLM \ } system \verb|\ current control \ } safe boot \verb|\ option| \\$ Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll

Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers

HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens kev: 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: ${\tt HKLM \ } system \verb|\ current control \verb|\ mui \ uilanguages \verb|\ len-us| \\$

Opens key: $\label{lem:hklmsystem} \verb|HKLM\| system \verb|\currentcontrolset\| control \verb|\mui\| uilanguages \verb|\pendingdelete|| \\$

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 HKCU\control panel\desktop\languageconfiguration Opens key: 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\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots Opens kev: HKCU\software\microsoft\windows nt\currentversion\appcompatflags Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions Opens key: $HKLM \verb|\software| \verb|\wow6432| node \verb|\policies| microsoft| windows nt \verb|\windows file| \\$ protection Opens key: HKLM\software\policies\microsoft\windows nt\windows file protection Opens key: HKLM\ Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\diagnostics Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\gre_initialize HKLM\software\wow6432node\microsoft\windows Opens key: nt\currentversion\compatibility32 $\label{lem:hklm} \mbox{HKLM\software\wow6432} node\mbox{\swindows nt\currentversion\swindows} \ \ \mbox{nt\currentversion\swindows} \ \ \mbox{\swindows} \ \mbox{\s$ Opens key: compatibility Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows 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\cmf\config Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\setup Opens key: HKLM\software\microsoft\windows\currentversion\setup Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale Opens key: HKLM\system\currentcontrolset\services\crypt32 Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet$ settings Opens kev: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder Opens key: HKLM\software\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: Opens key: HKCU\software\classes\ 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: $\label{lem:hkcu} \begin{tabular}{ll} HKCU software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\clsid| {20d04fe0-decomposition} {20d04fe$ 3aea-1069-a2d8-08002b30309d}\shellfolder Opens key: a2d8-08002b30309d}\shellfolder Opens key: HKCU\software\microsoft\windows\currentversion\policies\nonenum Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\nonenum Opens kev: 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\{8063a3d4-8213-11e3-a68e-806e6f6e6963}\ Opens key: HKCU\software\classes\drive\shellex\folderextensions Opens key: HKCR\drive\shellex\folderextensions HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-Opens key: 4442-804e-409d6c4515e9} Opens kev: 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\microsoft\windows\currentversion\explorer\
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced

HKCU\software\policies\microsoft\windows\explorer

HKCU\software\microsoft\windows\currentversion\explorer

Opens key:

Opens key:

Opens key:

 $HKLM \label{lem:hklm} Which is the last of the last$

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\directorv\

Opens key: HKCU\software\classes\directory\shellex\iconhandler

Opens key: HKCR\directory\shellex\iconhandler HKCU\software\classes\folder Opens kev:

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\directorv\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: ${\tt HKCR\ left} lesystem objects \ \verb|\ browseinplace| \\$ 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 kev: HKCU\software\classes\allfilesystemobjects\clsid

Opens key: HKCR\allfilesystemobjects\clsid

Opens key:

Opens kev:

db2c-424c-b029-7fe99a87c641}

Opens key:

db2c-424c-b029-7fe99a87c641}\propertybag

Opens key:

Opens key:

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders.

Opens key: HKLM\software\microsoft\com3

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

b8dc300d9f9d}

HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} Opens key: Opens key:

b8dc300d9f9d}\treatas

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

b8dc300d9f9d}\progid

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

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

b8dc300d9f9d}\progid

Opens key: $HKCR \c1sid \{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} \progid$

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprochandler32

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

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: HKLM\system\currentcontrolset\control\lsa\accessproviders

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

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ \ known folders ettings$

Opens kev:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{1b3ea5dc-1b4e$ b587-4786-b4ef-bd1dc332aeae}

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1b3ea5dc-b2442 node \ microsoft \ windows \ \ \ \ \}$ b587-4786-b4ef-bd1dc332aeae}\propertybag

Opens kev:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-40ex, \ baselines \$ 65f9-4cf6-a03a-e3ef65729f3d}

Opens key:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685db-16422 \\ node \setminus \{3eb68$ 65f9-4cf6-a03a-e3ef65729f3d}\propertybag

0e22-4760-9afe-ea3317b67173}

Opens kev:

0e22-4760-9afe-ea3317b67173}\propertybag

HKLM\software\wow6432node\microsoft\windows Opens key:

nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001

HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-Opens key: 980053277-1733835069-2361817685-1001

HKLM\software\wow6432node\microsoft\rpc Opens key:

 ${\tt HKLM \backslash system \backslash current control \backslash computer name \backslash active computer name}$ Opens key:

Opens key: HKLM\system\setup

HKLM\software\wow6432node\policies\microsoft\windows nt\rpc Opens kev:

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:

11e3-a68e-806e6f6e6963}\

Opens key: HKLM\software\wow6432node\evillyrics

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}

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

a0fb-4bfc-874a-c0f2e0b9fa8e}

Opens key:

a0fb-4bfc-874a-c0f2e0b9fa8e}\propertybag

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:

 $HKLM \ software \ wow 6432 node \ microsoft \ ctf \ compatibility \ 7842072 cea 4eb 57a 03b dd 00b 54088404. exemple \ description \ descrip$ Opens key:

Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436} Opens key: Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}

HKLM\software\wow6432node\microsoft\ctf\ Opens key:

Opens key: HKCU\software\microsoft\windows nt\currentversion\windows

Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink

Opens key: HKLM\software\microsoft\windows

nt\currentversion\languagepack\datastore_v1.0

HKLM\software\microsoft\windows Opens key:

nt\currentversion\languagepack\surrogatefallback

HKLM\software\microsoft\windows Opens key: nt\currentversion\languagepack\surrogatefallback\segoe ui HKLM\software\microsoft\windows Opens kev: nt\currentversion\languagepack\surrogatefallback\ms shell dlg 2

Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\ms shell dlg

HKLM\software\microsoft\windows nt\currentversion\image file execution Oueries value:

options[disableusermodecallbackfilter]

Queries value: HKLM\system\currentcontrolset\control\session

manager[cwdillegalindllsearch]

HKLM\system\currentcontrolset\control\terminal server[tsappcompat] Queries value: Oueries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]

Oueries value:

HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]

HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type] Queries value:

Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-

us[alternatecodepage]

Queries value: HKCU\control panel\desktop[preferreduilanguages] Oueries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest] Queries value: HKCU\software\microsoft\windows nt\currentversion\appcompatflags[showdebuginfo] HKLM\system\currentcontrolset\control\nls\sorting\versions[] Oueries value: HKLM\software\policies\microsoft\windows nt\windows file Queries value: protection[knowndlllist] HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Queries value: HKLM\software\microsoft\windows Oueries value: nt\currentversion\gre_initialize[disablemetafiles] HKLM\software\wow6432node\microsoft\windows Queries value: nt\currentversion\compatibility32[7842072cea4eb57a03bdd00b54088404] Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows[loadappinit dlls] Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap] Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Oueries value: HKLM\system\currentcontrolset\control\cmf\config[system] Queries value: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr[disable] Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath] HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us] HKLM\system\currentcontrolset\services\crypt32[debugheapflags] Oueries value: Queries value: settings[disableimprovedzonecheck] Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[security_hklm_only] Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel] Queries value: $HKLM \ software \ microsoft \ windows \ current version \ policies \ explorer [no set folders]$ HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon] Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups] $HKCR\wow6432 node\clsid\{20d04fe0-3aea-1069-a2d8-42d04fe0-3aea-42d04fe0-3aea$ Oueries value: 08002b30309d}\shellfolder[attributes] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\shellfolder[callforattributes] $HKCR \setminus wow 6432 \\ node \setminus clsid \setminus \{20d04fe0-3aea-1069-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1060-a2d8-4aea-1$ Queries value: 08002b30309d}\shellfolder[restrictedattributes] Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsfordisplay] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Queries value: 08002b30309d}\shellfolder[hidefolderverbs] Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[usedrophandler] Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsforparsing] $HKCR \verb|\wow6432| node \verb|\clsid| \{20d04fe0-3aea-1069-a2d8-4aea-1060-a2d8-4aea-10$ Oueries value: 08002b30309d}\shellfolder[wantsparsedisplayname] Oueries value: 08002b30309d}\shellfolder[queryforoverlay] Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[mapnetdriveverbs] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Queries value: 08002b30309d}\shellfolder[queryforinfotip] Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[hideinwebview] Oueries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[hideondesktopperuser] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\shellfolder[wantsaliasednotifications] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Queries value: $08002b30309d \verb|\shellfolder[wantsuniversaldelegate]|$ Oueries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[nofilefolderjunction] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[pintonamespacetree]

Queries value: HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-08002b30309d}]

Queries value:

08002b30309d}\shellfolder[hasnavigationenum]

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

Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d4-8213-11e3-a68e-806e6f6e6963}[data] Queries value: 11e3-a68e-806e6f6e6963}[generation] HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-Oueries value: 409d6c4515e9}[drivemask] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden] HKCU\software\microsoft\windows\currentversion\explorer[shellstate] Oueries value: Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess] Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling] HKLM\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenul Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext] $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{tabular} do not pretty path] \end{tabular}$ Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview] HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter] Queries value: Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling] $HKCU \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'advanced [autocheck select]$ Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay] HKCR\directory[docobject] Oueries value: HKCR\folder[docobject] Queries value: Queries value: HKCR\allfilesystemobjects[docobject] Queries value: HKCR\directory[browseinplace] Queries value: HKCR\folder[browseinplace] Oueries value: HKCR\allfilesystemobjects[browseinplace] Queries value: HKCR\directory[isshortcut] HKCR\folder[isshortcut] Oueries value: Queries value: HKCR\allfilesystemobjects[isshortcut] Queries value: HKCR\directory[alwaysshowext] Queries value: HKCR\directory[nevershowext] Queries value: HKCR\folder[nevershowext] HKCR\allfilesystemobjects[nevershowext] Queries value: db2c-424c-b029-7fe99a87c641}[category] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3adb2c-424c-b029-7fe99a87c641}[name] Oueries value: db2c-424c-b029-7fe99a87c641}[parentfolder] Oueries value: db2c-424c-b029-7fe99a87c641}[description]

db2c-424c-b029-7fe99a87c641}[relativepath]

db2c-424c-b029-7fe99a87c641}[parsingname]

Queries value:

Oueries value:

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

Queries value:

 $\label{localized} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\$

Queries value

 $\label{thm:local-problem} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folds \f$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3adb2c-424c-b029-7fe99a87c641\} [security]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3adb2c-424c-b029-7fe99a87c641\}[stream resource]$

Queries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3adb2c-424c-b029-7fe99a87c641\} \ [local redirectonly]$

Oueries value:

 $\label{thm:local-state} $HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}[roamable]}$

Queries value:

 $\label{thm:local-software-wow6432} HKLM\software-wow6432\\ node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma\begin{cases} b4bfcc3a-db2c-424c-b029-7fe99a87c641 \cite{b4bfcc3a-db2c-424c-b029-7fe99a87c641} \cite{b4bfcc3a-db2c-b029-7fe99a87c641} \cite{b4bfcc3a-db2c-b029-7fe99a87$

Queries value

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}[attributes]$

Oueries value:

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} [initfolder \ handler]$

 $\label{thm:linear} Queries \ value: \\ HKCU \ software \ microsoft \ windows \ current version \ (explorer \ windows). \\$

folders[desktop]

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

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

 $HKLM \setminus system \setminus current control \\ \setminus lsa \setminus access providers [martaextension]$

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:

Queries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [name]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[parent folder]$

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[description]

Queries value:

 $\label{thm:microsoftwindows} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\f(1b3ea5dc-b587-4786-b4ef-bd1dc332 aeae\}\[relative path]$

Queries value:

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [infotip]$

Queries value:

 $\label{localized halo} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \end{alized halo} \footnote{Alized ha$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [icon]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [security]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[stream resource]$

Oueries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [stream resource type]$

Oueries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} \ [local redirectonly]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [roamable]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[precreate]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[stream]$

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(1b3ea5dc-b587-4786-b4ef-bd1dc332aeae)\cite{hklmsoftware}\$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folds 6587-4786-b4ef-bd1dc332 aeae \end{cases} [attributes]$

Oueries value:

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [initfolder \ handler]$

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

folders[{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}]

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folds folder \folds \fo$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [name]$

Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folds folder \folder \folder \folds folder \folder \fold$

Queries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder 65f9-4cf6-a03a-e3ef65729f3d\folder$

Oueries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [relative path]$

Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folds folder \folds \fo$

Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folds \fo$

Queries value:

 $\label{localized halos of tware wow 6432 node in crosoft windows `current version `explorer `folder descriptions `\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[localized name]$

Queries value

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [security]$

Oueries value:

Queries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [local redirectonly]$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folds folder \folds \fo$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [precreate]$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folds folder \folds \fo$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [publish expanded path]$

Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folds \fo$

Oueries value:

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [initfolder handler]$

Queries value:

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

folders[appdata]

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \$

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\soft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[parentfolder]}$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{area} Hklm \en$

Oueries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [relative path]$

Oueries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsingname]

Queries value:

 $\label{lem:hklmsoftware} HKLM software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \f$

Queries value:

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

Oueries value:

 $\label{thm:local-substitution} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$

Queries value:

 $\label{lem:hklm} $HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[security]$$

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [stream resource type]$

Oueries value

 $\label{lem:hklmsoftware} HKLM software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \f$

Queries value:

 $\label{limits} $HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[roamable]}$

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [stream]$

Oueries value

 $\label{thm:local-basis} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1}{5}e6c858f-0e22-4760-9afe-ea3317b67173} [publish expanded path]$

Queries value:

 $\label{limit} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[attributes]}$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [folder type id]$

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1.00} \end{4.5} $$ (5e6c858f-0e22-4760-9afe-ea3317b67173) [initfolder handler] $$$

 $\label{lem:profile} Queries value: $$HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001[profileimagepath]$

Queries value: HKLM\software\microsoft\rpc[maxrpcsize]

Oueries value:

HKLM\system\currentcontrol\set\control\computername[computername]

Queries value: HKLM\system\setup[oobeinprogress]

Queries value: HKLM\system\setup[systemsetupinprogress]

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

Queries value:

 $\label{lem:hkculsoftware} HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ \{8063a3d3-8213-11e3-a68e-806e6f6e6963\} \ [data]$

Queries value:

 $\label{thm:local-condition} HKCU software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ \{8063a3d3-8213-11e3-a68e-806e6f6e6963\} \cline{200} \c$

Oueries value:

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

Oueries value:

 $\label{limit} $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\calebel{limit} $\{905e63b6-c1bf-494e-b29c-65b732d3d21a\}[name]$$

Oueries value:

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

Queries value:

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

Oueries value:

 $\label{lem:hklmsoftware} HKLM\software\wow6432\node\microsoft\windows\currentversion\explorer\folderdescriptions\end{4905e63b6-c1bf-494e-b29c-65b732d3d21a}[relative path]$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \gamma \folder \folder \folder \folder \folder \folder \folder \gamma \folder \fo$

Oueries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a\}[infotip]

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value

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

Queries value:

 $\label{thm:local} HKLM\software\wow6432 node\microsoft\windows\current version\explorer\folder descriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a\}[local redirectonly]}$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot\{905e63b6-c1bf-494e-b29c-65b732d3d21a\}\cdot{locality}\cdo$

Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \gamma \folder \f$

Queries value:

 $\label{limit} \begin{tabular}{ll} HKLM\software\wow6432\node\microsoft\windows\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\currentversion\explorer\currentversion\explorer\currentversion\explorer\currentversion\explorer\currentversion\explorer\currentversion\explorer\currentversion\explorer\currentversion\explorer\currentversion\explorer\currentversion\explorer\currentversion\explorer\currentversion\explorer\currentversion\explorer\currentversion\explorer\currentversion\explorer\currentversion\explorer\currentversion\explorer\explorer\currentversion\explorer\exp$

Queries value

 $\label{thm:local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a\}[publishexpandedpath]}$

Queries value:

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

Queries value:

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

Queries value:

 $\label{local-ham} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a\}[initfolderhandler]}$

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]

Queries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} [category]$

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1.5} a 0fb-4bfc-874a-c0f2e0b9fa8e \cite{1.5} [name]$

Queries value:

```
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-microsoft \ windows \ explorer \ folder \ descriptions \ explorer \ folder \ descriptions \ explorer \ folder \ descriptions \ explorer \ folder 
a0fb-4bfc-874a-c0f2e0b9fa8e}[parentfolder]
        Queries value:
HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-descriptions\} \\ for the first of the
a0fb-4bfc-874a-c0f2e0b9fa8e}[description]
a0fb-4bfc-874a-c0f2e0b9fa8e}[relativepath]
        Oueries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[parsingname]
        Oueries value:
HKLM \label{lem:hklm} Which was the statement of the st
a0fb-4bfc-874a-c0f2e0b9fa8e}[infotip]
        Queries 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]
        Queries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresource]
HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-descriptions\} \\ for the first of the
a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresourcetype]
        Oueries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[localredirectonly]
        Oueries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[roamable]
        Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{7c5a40ef-microsoft \ windows \ explorer \ folder \ descriptions \ \ \ \}
a0fb-4bfc-874a-c0f2e0b9fa8e}[precreate]
a0fb-4bfc-874a-c0f2e0b9fa8e}[stream]
        Queries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[publishexpandedpath]
        Oueries value:
```

a0fb-4bfc-874a-c0f2e0b9fa8e}[attributes]

Queries value:

a0fb-4bfc-874a-c0f2e0b9fa8e}[foldertypeid]

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{7c5a40effolder \ and \ baselines \ and \ and \ baselines \ and \ and \ baselines \ and \ and$ a0fb-4bfc-874a-c0f2e0b9fa8e}[initfolderhandler]

a0fb-4bfc-874a-c0f2e0b9fa8e}\propertybag[foldersdependenton]

HKLM\system\currentcontrolset\control\nls\locale[00000409] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1] Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable] Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]

Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[scrollinset] $\label{lem:hkcu} \verb+KKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]$ Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist] Oueries value: Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[scrolldelay]

HKCU\software\microsoft\windows Queries value:

nt\currentversion\windows[scrollinterval]

Oueries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\datastore_v1.0[disable] HKLM\software\microsoft\windows Queries value: nt\currentversion\languagepack\datastore_v1.0[datafilepath] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane1] Oueries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane2]

HKLM\software\microsoft\windows Oueries value: nt\currentversion\languagepack\surrogatefallback[plane3]

HKLM\software\microsoft\windows Queries value: nt\currentversion\languagepack\surrogatefallback[plane4]

Queries value: HKLM\software\microsoft\windows $\verb|nt\currentversion\language| pack\surrogatefallback[plane5]|$

Queries value: HKLM\software\microsoft\windows $\verb|nt\currentversion\language| pack\surrogatefallback[plane6]|$ Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane7] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane8] HKLM\software\microsoft\windows Queries value: nt\currentversion\languagepack\surrogatefallback[plane9] HKLM\software\microsoft\windows Oueries value: nt\currentversion\languagepack\surrogatefallback[plane10] HKLM\software\microsoft\windows Queries value: $\verb|nt\currentversion\language| pack\surrogatefallback[plane11]|$ Queries value: HKLM\software\microsoft\windows $\verb|nt\currentversion\languagepack\surrogatefallback[plane12]|$ Queries value: HKLM\software\microsoft\windows $\verb|nt\currentversion\languagepack\surrogatefallback[plane13]|$ Queries value: HKLM\software\microsoft\windows $\verb|nt\currentversion\languagepack\surrogatefallback[plane14]|$ HKLM\software\microsoft\windows Oueries value: nt\currentversion\languagepack\surrogatefallback[plane15] HKLM\software\microsoft\windows Oueries value: $\verb|nt\currentversion\language| pack\surrogatefallback[plane16]|$ Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]|$