Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 31, Task ID: 124

Task ID: 124

Risk Level: 4

Date Processed: 2016-04-28 12:50:30 (UTC)

Processing Time: 61.12 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\bd9521b80b08a3c77a5f60c04f2adfe0.exe"

Sample ID: 31 Type: basic Owner: admin

Label: bd9521b80b08a3c77a5f60c04f2adfe0

Date Added: 2016-04-28 12:44:52 (UTC)

File Type: PE32:win32:gui File Size: 773509 bytes

MD5: bd9521b80b08a3c77a5f60c04f2adfe0

SHA256: 5b4ba521e77f896256818f3e5b5a8bf1f0d499a25475b69545ef71d963ef9ce7

Description: None

Pattern Matching Results

2 PE: Nonstandard section

4 Packer: NSIS [Nullsoft Scriptable Install System]

Static Events

Anomaly: PE: Contains a virtual section

Anomaly: PE: Contains one or more non-standard sections

Process/Thread Events

Creates process: C:\windows\temp\bd9521b80b08a3c77a5f60c04f2adfe0.exe

["C:\windows\temp\bd9521b80b08a3c77a5f60c04f2adfe0.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0

Creates mutex: \Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1

Creates event: \KernelObjects\MaximumCommitCondition

File System Events

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

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

Creates: C:\Users\Admin\AppData\Local\Temp\nse1586.tmp

Opens: C:\Windows\Prefetch\BD9521B80B08A3C77A5F60C04F2AD-EE833139.pf

Opens: C:\Windows

 Opens:
 C:\Windows\System32\wow64.dl1

 Opens:
 C:\Windows\System32\wow64win.dl1

 Opens:
 C:\Windows\System32\wow64cpu.dl1

 Opens:
 C:\Windows\system32\wow64log.dl1

Opens: C:\Windows\SysWOW64

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

Opens: C:\windows\temp\bd9521b80b08a3c77a5f60c04f2adfe0.exe.Local\

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

 $\label{lem:controls} Opens: C:\<list-item>\windows\\ \winsxs\\ \xse_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\\ \comctl32.dll$

Opens: C:\windows\temp\VERSION.dll
Opens: C:\Windows\SysWOW64\version.dll
Opens: C:\Windows\SysWOW64\imm32.dll
Opens: C:\Windows\SysWOW64\rpcss.dll
Opens: C:\Windows\SysWOW64\uxtheme.dll
Opens: C:\windows\temp\SHFOLDER.DLL
Opens: C:\Windows\SysWOW64\shfolder.dll

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

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

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

 $controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2$

Opens: C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll

Opens: C:\Windows\WindowsShell.Manifest

Opens: C:\

Opens: C:\Windows\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

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

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

Opens: C:\Users\Admin\Desktop\desktop.ini
Opens: C:\windows\temp\profapi.dll
Opens: C:\Windows\SysWOW64\profapi.dll
Opens: C:\Users\Admin\AppData\Local\Temp

Opens: C:\Users\Admin\AppData\Local\Temp\nse1586.tmp
Opens: C:\Windows\Temp\bd9521b80b08a3c77a5f60c04f2adfe0.exe

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

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

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

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

Opens: C:\Program Files (x86)

Opens: C:\Program Files (x86)\Outlook Serienmail 3

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

Opens: C:\Program Files (x86)\Common Files\microsoft shared\ink\tiptsf.dll

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

Reads from: C:\Windows\Temp\bd9521b80b08a3c77a5f60c04f2adfe0.exe

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

Deletes: C:\Users\Admin\AppData\Local\Temp\nse1586.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 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\currentcontrol\set\control\mui\settings\languageconfiguration
Opens key: HKCU\software\policies\microsoft\control panel\desktop

Opens key. HKCU\ control | nanel\ deskton\ language aconfiguration

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:

Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions

Opens key: HKLM\

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

nt\currentversion\diagnostics

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\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:

Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer

 $Opens\;key: \\ \qquad \qquad \text{HKLM} \\ system \\ \text{current control } \\ \text{nls} \\ \text{extended locale}$

Opens key:

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

Opens key: HKCU\software\classes\

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

08002b30309d}\shellfolder

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

08002b30309d}\shellfolder

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-

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

Opens key:

a2d8-08002b30309d}\shellfolder

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

Opens key:

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

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

Opens kev:

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

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 HKCU\software\policies\microsoft\windows\explorer Opens key: HKCU\software\microsoft\windows\currentversion\explorer Opens kev: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced

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\directory\

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

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

Opens key: HKCR\folder

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

HKCR\folder\shellex\iconhandler Opens key:

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 kev: HKCU\software\classes\folder\docobject

Opens key: HKCR\folder\docobject

Opens key: HKCU\software\classes\allfilesystemobjects\docobject

Opens key: HKCR\allfilesystemobjects\docobject

Opens key: HKCU\software\classes\directory\browseinplace

Opens key: HKCR\directory\browseinplace

Opens key: HKCU\software\classes\folder\browseinplace

HKCR\folder\browseinplace Opens key:

Opens key: HKCU\software\classes\allfilesystemobjects\browseinplace

Opens key: HKCR\allfilesystemobjects\browseinplace Opens key: HKCU\software\classes\directory\clsid

Opens key: HKCR\directory\clsid

Opens key: HKCU\software\classes\folder\clsid

Opens key: HKCR\folder\clsid

Opens key: HKCU\software\classes\allfilesystemobjects\clsid

Opens key: HKCR\allfilesystemobjects\clsid

Opens key:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{b4bfcc3a-b4bf$

db2c-424c-b029-7fe99a87c641}

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ f$

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

HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1 Opens kev:

Opens key:

 $\label{thm:local_hammon} HKCU \software \microsoft \windows \current version \explorer \session in folders$

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}

Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\treatas Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\progid Opens key: $HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid$ Opens key: HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} Opens key: HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\progid HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid Opens kev: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Opens key: b8dc300d9f9d}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\inprocserver32 Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\inprochandler32 HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Opens key: b8dc300d9f9d}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Opens key: b8dc300d9f9d}\inprochandler Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\inprochandler Opens key: HKLM\system\currentcontrolset\control\lsa\accessproviders Opens key: HKLM\system\currentcontrolset\services\ldap Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings Opens key: b587-4786-b4ef-bd1dc332aeae} b587-4786-b4ef-bd1dc332aeae}\propertybag Opens key: 65f9-4cf6-a03a-e3ef65729f3d} Opens key:

65f9-4cf6-a03a-e3ef65729f3d}\propertybag

Opens key:

0e22-4760-9afe-ea3317b67173}

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{5e6c858f-4c41\} \\ for the first of the first o$ 0e22-4760-9afe-ea3317b67173}\propertybag

Opens key: HKLM\software\wow6432node\microsoft\windows $nt \verb|\currentversion| profile list \verb|\s-1-5-21-980053277-1733835069-2361817685-1001| list list \verb|\s-1-5-21-980053277-1733885-1001| list \verb|\s-1-5-21-98005327-1001| list \verb|\s-1-5-21-9800$

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

980053277-1733835069-2361817685-1001

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\wow6432node\microsoft\windows\currentversion

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

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

HKLM\system\setup Opens key:

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

Opens key: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKLM\software\policies\microsoft\sqmclient\windows

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

HKLM\software\wow6432node\osm Opens key:

Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-11e3-a68e-806e6f6e6963}\

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:

Opens key: $HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus ctf \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - b$

Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436} $HKLM \setminus software \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07 - be18 - b$ Opens kev: $0 fb 58b 01c 4a 4 \\ 1 anguage profile \\ 0x 00 00 00 00 \\ 10 00 1 be a 3-ed 56-48 3d-a 2e 2-a ea e 25577436 \\ 1 anguage profile \\ 1 anguage \\ 1 anguage profile \\ 1 anguage \\$

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

Opens key: $\label{lem:hklm} \mbox{HKLM\software\mbox{\sc microsoft\windows} nt\current version\sc fontlink\systemlink} \\$

Opens key: HKLM\software\microsoft\windows

nt\currentversion\languagepack\datastore_v1.0

HKLM\software\microsoft\windows Opens key:

nt\currentversion\languagepack\surrogatefallback

Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\ms shell dlg 2 HKLM\software\wow6432node\policies Opens kev: Opens key: HKCU\software\policies Opens key: HKCU\software Opens key: HKLM\software\wow6432node Opens key: $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \explorer \autocomplete \end{tabular}$ HKCU\software\microsoft\windows\currentversion\explorer\autocomplete Opens key: Opens key: HKLM\software\policies\microsoft\windows\currentversion\explorer\autocomplete Opens key: Opens key: 00c04fd7d062} Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062} Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\treatas HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\treatas Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\progid Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\progid HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062} Opens key: Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062} Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\progid Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\progid Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32 Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandler32 HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-Opens kev: 00c04fd7d062}\inprochandler32 Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandler HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-Opens key: 00c04fd7d062}\inprochandler Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{03c036f1-a186-11d0-824a-b140-$ 00aa005b4383} HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-. 00aa005b4383}\treatas Opens key: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\treatas Opens key: HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\progid Opens key: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\progid Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-00aa005b4383} Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383} Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\progid Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\progid $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{03c036f1-a186-11d0-824a-11d0-$ Opens key: 00aa005b4383}\inprocserver32 HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-Opens key: 00aa005b4383}\inprocserver32 $HKCU \setminus software \setminus classes \setminus wow 6432 node \setminus clsid \setminus \{03c036f1-a186-11d0-824a-11d0-82$ Opens key: 00aa005b4383}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprochandler32 $HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{03c036f1-a186-11d0-824a-11d0-8$ Opens key: 00aa005b4383}\inprochandler HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-Opens key: 00aa005b4383}\inprochandler Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062} Opens key: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062} Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treatas $\label{lower} HKCR \land wow6432 node \clsid \end{c1} Idd-a535-00c04fd7d062 \treat as$ Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\progid Opens key: $HKCR \ wow 6432 node \ clsid \ \{00bb2763-6a77-11d0-a535-00c04fd7d062\} \ \ progid$ Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062} Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062} Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\progid Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\progid Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-Opens key: 00c04fd7d062}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandler32 Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandler HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-Opens key: 00c04fd7d062}\inprochandler Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete\client\ Opens kev: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920b61bb7cdd997} HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920b61bb7cdd997}\treatas Opens key: $HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997\}\treatas$ Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920b61bb7cdd997}\progid Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\progid Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920b61bb7cdd997}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920b61bb7cdd997}\inprocserver32 Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920b61bb7cdd997}\inprochandler32 HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-Opens key: b61bb7cdd997}\inprochandler32 Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920b61bb7cdd997}\inprochandler Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920b61bb7cdd997}\inprochandler Opens key: HKLM\software\wow6432node\microsoft\rpc\extensions Opens key: HKLM\software\microsoft\rpc\extensions Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\fontsubstitutes Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\segoe ui HKLM\software\microsoft\windows nt\currentversion\image file execution Oueries value: options[disableusermodecallbackfilter] Queries value: HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch] Oueries 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] Oueries value: HKLM\system\currentcontrolset\control\mui\uilanguages\enus[alternatecodepage] Queries value: HKCU\control panel\desktop[preferreduilanguages] HKCU\control panel\desktop\muicached[machinepreferreduilanguages] Queries value: Queries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [prefer external manifest]$ Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[] HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Oueries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles] HKLM\software\wow6432node\microsoft\windows Oueries value: nt\currentversion\compatibility32[bd9521b80b08a3c77a5f60c04f2adfe0] Oueries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows[loadappinit_dlls] HKLM\software\microsoft\ole[pageallocatorusesystemheap] Oueries value: Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer] HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin] Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders] Oueries value:

Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us] Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups] Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[attributes]

HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]

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

```
Oueries value:
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[callforattributes]
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries value:
08002b30309d}\shellfolder[restrictedattributes]
 Queries value:
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsfordisplay]
 Oueries value:
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hidefolderverbs]
 Oueries value:
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[usedrophandler]
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Oueries value:
08002b30309d}\shellfolder[wantsforparsing]
 Queries value:
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsparsedisplayname]
 Queries value:
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforoverlay]
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries value:
08002b30309d}\shellfolder[mapnetdriveverbs]
 Oueries value:
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforinfotip]
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Oueries value:
08002b30309d}\shellfolder[hideinwebview]
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries value:
08002b30309d}\shellfolder[hideondesktopperuser]
 Oueries value:
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsaliasednotifications]
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries value:
08002b30309d}\shellfolder[wantsuniversaldelegate]
 Queries value:
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[nofilefolderjunction]
 Oueries value:
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[pintonamespacetree]
                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Oueries value:
08002b30309d}\shellfolder[hasnavigationenum]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}1
 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]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
                        HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
 Queries value:
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
                        HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
 Oueries value:
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
 Queries value:
Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
                        HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
 Oueries value:
 Queries 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 \ current version \ explorer \ advanced [nonetcrawling]
 Oueries value:
```

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]

Queries value: HKCR\directory[docobject]
Queries value: HKCR\folder[docobject]

Queries value: HKCR\allfilesystemobjects[docobject]
Queries value: HKCR\directory[browseinplace]
Queries value: HKCR\folder[browseinplace]

Queries value: HKCR\allfilesystemobjects[browseinplace]

Queries value: HKCR\directory[isshortcut]
Queries value: HKCR\folder[isshortcut]

Queries value: HKCR\allfilesystemobjects[isshortcut]
Queries value: HKCR\directory[alwaysshowext]
Queries value: HKCR\directory[nevershowext]
Queries value: HKCR\folder[nevershowext]

Queries value: HKCR\allfilesystemobjects[nevershowext]

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\folde$

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries 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\gamma\folderdescriptions\gamma\$

Oueries value:

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

Queries value:

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

Queries value:

Queries value:

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma_{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[streamresourcetype]$

Oueries value:

 $\label{local-continuous} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder des$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}[roamable]$

Queries value

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma_{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[publishexpandedpath]$

Queries value:

 $\label{thm:local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \begin{tabular}{l} b4bfcc3a-db2c-424c-b029-7fe99a87c641} [attributes] \end{tabular}$

Queries value:

 $\label{limit} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder descriptions\folder descriptions\folder\fold$

Queries value:

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

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

folders[desktop]

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

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: HKLM\software\microsoft\ole[maxsxshashcount]

Oueries value:

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

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

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

Queries value: HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]

Queries value:

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

Oueries 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:

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

Oueries value:

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

Queries value:

 $\label{thm:local-basis} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1} b587-4786-b4ef-bd1dc332 aeae \cite{1} [parsing name]$

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

Queries value:

 $\label{localized-holder} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\f(1b3ea5dc-b587-4786-b4ef-bd1dc332aeae)\f(1calredirectonly)\f(1calredi$

Queries value:

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

Queries value:

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

Queries value:

 $H\dot{L}M\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[stream]

Queries value:

 $\label{local-prop} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332eae\}[publishexpandedpath]}$

Queries value:

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

Oueries value:

 $\label{thm:hammon} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \fill 1b3ea5dc-b587-4786-b4ef-bd1dc332aeae \folder typeid \fill 1b3ea5dc-b587-4786-b4ef-bd1dc332aeae \folder \fo$

Queries value:

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

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432} HKLM \software \wow6432 node \windows \current version \explorer \folder descriptions \eqref 65f9-4cf6-a03a-e3ef65729f3d \eqref [name]$

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklm} HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [folder type id]$

Queries value:

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

Queries value:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$microsoft \windows \current version \explorer \substitutes} \end{tabular} \begin{tabular}{ll} explorer \mbox{$microsoft \windows \current version \explorer \substitutes} \end{tabular} \begin{tabular}{ll} explorer \mbox{$microsoft \windows \current version \explorer \substitutes} \end{tabular} \begin{tabular}{ll} explorer \mbox{$microsoft \windows \current version \explorer \substitutes} \end{tabular} \begin{tabular}{ll} explorer \mbox{$microsoft \windows \current version \explorer \substitutes} \end{tabular} \begin{tabular}{ll} explorer \mbox{$microsoft \windows \current \windows \explorer \explorer \explorer \explorer \windows \explorer \exp$

folders[appdata]

Oueries 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-ham} $$HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[parentfolder]$$$

Queries value:

 $\label{thm:local-ham} $$HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[description]}$

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

```
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{5e6c858f-explorer\} \ folder \ before \ folder \ folder \ before \ folder \ folde
0e22-4760-9afe-ea3317b67173}[icon]
    Queries value:
0e22-4760-9afe-ea3317b67173}[security]
0e22-4760-9afe-ea3317b67173}[streamresource]
    Oueries value:
0e22-4760-9afe-ea3317b67173}[streamresourcetype]
    Oueries value:
HKLM \label{lem:hklm} Which was the statement of the second of the sec
0e22-4760-9afe-ea3317b67173}[localredirectonly]
0e22-4760-9afe-ea3317b67173}[roamable]
    Oueries value:
0e22-4760-9afe-ea3317b67173}[precreate]
    Oueries value:
0e22-4760-9afe-ea3317b67173}[stream]
    Queries value:
0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[attributes]
    Queries value:
0e22-4760-9afe-ea3317b67173}[foldertypeid]
    Oueries value:
0e22-4760-9afe-ea3317b67173}[initfolderhandler]
    Oueries value:
                                                        HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
980053277-1733835069-2361817685-1001[profileimagepath]
    Queries value:
                                                        HKLM\system\currentcontrolset\control\cmf\config[system]
                                                        HKLM\software\wow6432node\microsoft\windows\windows error
    Queries value:
reporting\wmr[disable]
    Queries value:
                                                        HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
    Queries value:
                                                        HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
    Oueries value:
                                                        HKLM\software\microsoft\rpc[maxrpcsize]
HKLM\system\currentcontrolset\control\computername[computername]
                                                        HKLM\system\setup[oobeinprogress]
    Queries value:
    Queries value:
                                                        HKLM\system\setup[systemsetupinprogress]
    Queries value:
                                                        HKLM\software\microsoft\sqmclient\windows[ceipenable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]
11e3-a68e-806e6f6e6963}[data]
    Queries value:
\label{local-prop} HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ \{8063a3d3-8213-646464, \mountpoints 2 \cpc \volume \ \{8063a3d3-8213-64646, \mountpoints 2 \cpc \volume \ \} \ \mountpoints \mou
11e3-a68e-806e6f6e6963}[generation]
                                                        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]
                                                        HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\languagepack\datastore_v1.0[disable]
                                                        HKLM\software\microsoft\windows
    Oueries value:
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
                                                        HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\languagepack\surrogatefallback[plane1]
    Oueries value:
                                                        HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
                                                        HKLM\software\microsoft\windows
    Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane3]|
    Queries value:
                                                        HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
    Oueries value:
                                                        HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
```

HKLM\software\microsoft\windows

HKLM\software\microsoft\windows

HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback[plane6]

nt\currentversion\languagepack\surrogatefallback[plane7]

nt\currentversion\languagepack\surrogatefallback[plane8]

Oueries value:

Queries value:

Queries value:

```
HKLM\software\microsoft\windows
 Oueries value:
\verb|nt\currentversion\language| pack\surrogatefallback[plane9]|
                          HKLM\software\microsoft\windows
 Queries value:
\verb|nt\currentversion\language| pack\surrogatefallback[plane10]|
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
 Queries value:
                          HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback[plane12]|
                          HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane13]
                          HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane14]
 Queries value:
                          HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback[plane15]|
                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[append completion]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]
 Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
 Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete[always use tabl
                          HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}[]
 Queries value:
                          HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
 Oueries value:
00c04fd7d062}\inprocserver32[inprocserver32]
                         HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
 Queries value:
00c04fd7d062}\inprocserver32[]
                          HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
 Queries value:
00c04fd7d062}\inprocserver32[threadingmodel]
 Queries value:
                          HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}[]
                          HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
 Oueries value:
00aa005b4383}\inprocserver32[inprocserver32]
                         HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
 Queries value:
00aa005b4383}\inprocserver32[]
                          HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
 Queries value:
00aa005b4383}\inprocserver32[threadingmodel]
 Queries value:
                          HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}[]
 Queries value:
                          HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
                          HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
 Oueries value:
00c04fd7d062}\inprocserver32[]
 Queries value:
                          HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete\client[]
                          HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\progid[]
 Oueries value:
                          HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}[]
 Queries value:
                          HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
 Oueries value:
b61bb7cdd997}\inprocserver32[inprocserver32]
                          HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
 Queries value:
b61bb7cdd997}\inprocserver32[]
 Queries value:
                          HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32[threadingmodel]
 Queries value:
                          HKLM\software\microsoft\rpc\extensions[ndroleextdll]
 Queries value:
                          HKCU\control panel\desktop[smoothscroll]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewalphaselect]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[acclistviewv6]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe
ui]
```