Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 42, Task ID: 165

Task ID: 165

Risk Level: 4

Date Processed: 2016-04-28 12:51:31 (UTC)

Processing Time: 2.38 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\fec00c2e3361c5caf7382f9ea1a7442f.exe"

Sample ID: 42 Type: basic Owner: admin

Label: fec00c2e3361c5caf7382f9ea1a7442f

Date Added: 2016-04-28 12:44:54 (UTC)

File Type: PE32:win32:gui File Size: 193824 bytes

MD5: fec00c2e3361c5caf7382f9ea1a7442f

SHA256: 153a3296a523ae0f606dfb4cb4178affe97e2f7c4f1faab223ca653e5b74261c

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\fec00c2e3361c5caf7382f9ea1a7442f.exe

["C:\windows\temp\fec00c2e3361c5caf7382f9ea1a7442f.exe"]

Terminates process: C:\Windows\Temp\fec00c2e3361c5caf7382f9ea1a7442f.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

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

Creates: C:\Users\Admin\AppData\Local\Temp\nsz2B7B.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\nsz2BCA.tmp

Creates: C:\Users
Creates: C:\Users\Admin
Creates: C:\Users\Admin\AppData
Creates: C:\Users\Admin\AppData\Lo

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

Creates: C:\Program Files (x86)

Creates: C:\Program Files (x86)\Mozilla Maintenance Service
Creates: C:\Users\Admin\AppData\Local\Temp\nsz2BCA.tmp\nsExec.dll

Creates: C:\Program Files (x86)\Mozilla Maintenance Service\Uninstall.exe
Opens: C:\Windows\Prefetch\FEC00C2E3361C5CAF7382F9EA1A74-D2300A69.pf

Opens: C:\Windows

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

Opens: C:\Windows\SysWOW64

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

Opens: C:\Windows\Temp\fec00c2e3361c5caf7382f9ea1a7442f.exe

Opens: C:\Windows\SysWOW64\ntdll.dll
Opens: C:\Windows\SysWOW64\kernel32.dll
Opens: C:\Windows\SysWOW64\KernelBase.dll
Opens: C:\Windows\apppatch\sysmain.sdb

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

controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985

 $\label{lem:controls} Opens: C: \windows \winSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\\\comctl32.dl1$

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

Opens: C:\Windows\SysWOW64\cryptbase.dll
Opens: C:\Windows\SysWOW64\sspicli.dll
Opens: C:\Windows\SysWOW64\rpcrt4.dll

Opens: C:\Windows\SysWOW64\shlwapi.dll C:\Windows\SysWOW64\shell32.dll Opens: C:\Windows\SysWOW64\advapi32.dll Opens: Opens: C:\Windows\SysWOW64\ole32.dll C:\Windows\SysWOW64\imm32.dll Opens: Opens: C:\Windows\SysWOW64\msctf.dll Opens: C:\Windows\WindowsShell.Manifest Opens: C:\Windows\SysWOW64\oleaut32.dll Opens: C:\Windows\SysWOW64\uxtheme.dll C:\Windows\SysWOW64\shfolder.dll Opens: C:\Windows\SysWOW64\SHCore.dll Opens:

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

Opens: C:\

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

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

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

 Opens:
 C:\Windows\SysWOW64\desktop.ini

 Opens:
 C:\Users\Admin\Desktop\desktop.ini

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

Opens: C:\Users\Admin\AppData\Local\Temp\nsz2B7B.tmp

Opens: C:\Windows\SysWOW64\cfgmgr32.dl1
Opens: C:\Windows\SysWOW64\devobj.dl1
Opens: C:\Windows\SysWOW64\setupapi.dl1
Opens: C:\Users\Admin\AppData\Local\Temp

Opens: C:\Users\Admin\AppData\Local\Temp\nsz2BCA.tmp

Opens: C:\Users\Admin\AppData\Local\Temp\nsz2BCA.tmp\System.dll
Opens: C:\Program Files (x86)\Mozilla Maintenance Service

Opens: C:\Windows\Temp

Opens: C:\Users\Admin\AppData\Local\Temp\nsz2BCA.tmp\nsExec.dll

Opens: C:\Program Files (x86)\Mozilla Maintenance Service\Uninstall.exe\
Opens: C:\Program Files (x86)\Mozilla Maintenance Service\Uninstall.exe

Opens: C:\Users\Admin\AppData\Local
Opens: C:\Users\Admin\AppData

Opens: C:\Users\Admin

Opens: C:\Users

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

Reads from: C:\Windows\Temp\fec00c2e3361c5caf7382f9ea1a7442f.exe
Deletes: C:\Users\Admin\AppData\Local\Temp\nsz2B7B.tmp
Deletes: C:\Users\Admin\AppData\Local\Temp\nsz2BCA.tmp

Deletes: C:\Users\Admin\AppData\Local\Temp\nsz2BCA.tmp\nsExec.dll
Deletes: C:\Users\Admin\AppData\Local\Temp\nsz2BCA.tmp\System.dll

Windows Registry Events

Creates key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ uninstall \ mozilla maintenance service$

Creates key: HKLM\software\mozilla\maintenanceservice

Creates key: HKLM\software
Creates key: HKLM\software\mozilla

Deletes value: HKLM\software\mozilla\maintenanceservice[ffprefetchdisabled]

Opens key: HKLM\software\microsoft\wow64

 $\label{lem:control} 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\currentcontrol\nls\customlocale
Opens key: HKLM\system\currentcontrol\st\language
Opens key: HKLM\system\currentcontrol\st\control\mui\uilanguages
Opens key: HKLM\system\currentcontrol\st\control\mui\uilanguages\en-us

 $Opens\ key: \\ HKLM\system\currentcontrolset\control\mui\anguages\pending delete$

Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings

Opens key: HKLM\software\policies\microsoft\mui\settings

Opens key: HKCU\

Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration

Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop\languageconfiguration

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

 $Opens~key: \\ HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside$

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\disable8and16bitmitigation

Opens key:

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

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

execution options

HKLM\software\microsoft\windows nt\currentversion\image file execution options

Opens key:

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

options\dllnxoptions

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

nt\currentversion\gre_initialize

Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize

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

nt\currentversion\compatibility32

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime

compatibility

Opens key:

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

Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy

Opens key: HKLM\system\currentcontrolset\control\lsa

Opens key:

HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration

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

Opens key: HKLM\software\microsoft\ole

Opens key: HKLM\software\wow6432node\microsoft\ole\tracing

Opens key: HKLM\software\microsoft\ole\tracing

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

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

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

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer

Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ fec 00c 2e 3361c 5 caf 7382 f 9e a 1a 7442 f. exellowed by the compatibility of the compatibility \ application \ fec 00c 2e 3361c 5 caf 7382 f 9e a 1a 7442 f. exellowed \ by the compatibility \ application \ fec 00c 2e 3361c 5 caf 7382 f 9e a 1a 7442 f. exellowed \ by the compatibility \ application \ fec 00c 2e 3361c 5 caf 7382 f 9e a 1a 7442 f. exellowed \ by the compatibility \ application \ fec 00c 2e 3361c 5 caf 7382 f 9e a 1a 7442 f. exellowed \ by the compatibility \ application \ fec 00c 2e 3361c 5 caf 7382 f 9e a 1a 7442 f. exellowed \ by the compatibility \ application \ fec 00c 2e 3361c 5 caf 7382 f 9e a 1a 7442 f. exellowed \ by the compatibility \ application \ fec 00c 2e 3361c 5 caf 7382 f 9e a 1a 7442 f. exellowed \ by the compatibility \ application \ fec 00c 2e 3361c 5 caf 7382 f 9e a 1a 7442 f. exellowed \ by the compatibility \ application \ fec 00c 2e 3361c 5 caf 7382 f 9e a 1a 7442 f. exellowed \ by the compatibility \ application \ fec 00c 2e 3361c 5 caf 7382 f 9e a 1a 7442 f. exellowed \ by the compatibility \ application \ fec 00c 2e 3361c 5 caf 7382 f. exellowed \ application \ fec 00c 2e 3361c 5 caf 7382 f. exellowed \ application \ fec 00c 2e 3361c 5 caf 7382 f. exellowed \ application \ fec 00c 2e 3361c 5 caf 7382 f. exellowed \ application \ fec 00c 2e 3361c 5 caf 7382 f. exellowed \ application \ fec 00c 2e 3361c 5 caf 7382 f. exellowed \ application \ fec 00c 2e 3361c 5 caf 7382 f. exellowed \ application \ fec 00c 2e 3361c 5 caf 7382 f. exellowed \ application \ fec 00c 2e 3361c 5 caf 7382 f. exellowed \ application \ fec 00c 2e 3361c 5 caf 7382 f. exellowed \ application \ fec 00c 2e 3361c 5 caf 7382 f. exellowed \ application \ appl$

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

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:

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

Opens key:

a2d8-08002b30309d}\shellfolder

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

Opens key:

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

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

08002b30309d}\inprocserver32

Opens key:

11e3-be65-806e6f6e6963}\

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

Opens key: HKCR\drive\shellex\folderextensions

Opens key: HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-

4442-804e-409d6c4515e9}

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

409d6c4515e9}

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

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

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

Opens key: HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-

97a27216f98a}\inprocserver32

Opens key: HKCU\software\classes\directory

Opens kev: HKCR\directory

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

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

Opens key: HKCR\folder

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

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 HKCR\allfilesystemobjects\docobject Opens key: Opens key: HKCU\software\classes\directory\browseinplace Opens key: HKCR\directory\browseinplace Opens kev: HKCU\software\classes\folder\browseinplace Opens key: HKCR\folder\browseinplace HKCU\software\classes\allfilesystemobjects\browseinplace Opens key: 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: HKCR\wow6432node\clsid\{75847177-f077-4171-bd2ca6bb2164fbd0}\inprocserver32 Opens key: HKLM\software\microsoft\com3 HKLM\software\microsoft\windowsruntime\clsid Opens kev: Opens key: b8dc300d9f9d} Opens key: HKCR\activatableclasses\clsid Opens key: HKCR\activatableclasses\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Opens key: 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 HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Opens key: b8dc300d9f9d}\inprocserver32 HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Opens key: b8dc300d9f9d}\inprocserver32 Opens kev: b8dc300d9f9d}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\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: Opens key: db2c-424c-b029-7fe99a87c641} Opens key: db2c-424c-b029-7fe99a87c641}\propertybag $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus session in fo \setminus 1$ Opens key: $HKCU \ software \ microsoft \ windows \ current version \ explorer \ session info \ 1\ known folders$ Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ known foldersettings$ $HKLM \label{lem:hklm} Which was the statement of the second of the sec$ b587-4786-b4ef-bd1dc332aeae} Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-part \ and \ barrier \ barr$ b587-4786-b4ef-bd1dc332aeae}\propertybag Opens key:

65f9-4cf6-a03a-e3ef65729f3d}

Opens key:

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

0e22-4760-9afe-ea3317b67173}

Opens key:

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

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

```
nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001
    Opens kev:
                                                          HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1923240461-1905901954-2556564120-1001
    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
                                                          HKLM\software\wow6432node\microsoft\windows\currentversion
    Opens key:
    Opens key:
                                                          HKLM \ system \ current control \ device classes \ \ \{53f5630d-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b
94f2-00a0c91efb8b}
    Opens key:
                                                          HKLM \ system \ current control \ device classes \ \ \{53f5630d-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b
94f2-00a0c91efb8b}\properties
    Opens kev:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mountpoints 2 \setminus cpc \setminus volume \setminus \{d5291c63-7c88-d124, d244, d24
11e3-be65-806e6f6e6963}\
    Opens key:
                                                          HKLM\software\wow6432node\mozilla\maintenanceservice
    Opens key:
                                                          HKLM\software\mozilla\maintenanceservice
    Opens key:
                                                          HKLM\software\wow6432node\microsoft\rpc\extensions
    Opens key:
                                                          HKLM\software\microsoft\rpc\extensions
    Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
                                                          HKLM\system\currentcontrolset\control\nls\customlocale[empty]
    Oueries value:
    Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
    Queries value:
                                                          HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
                                                          HKLM\system\currentcontrolset\control\mui\uilanguages\en-
    Oueries value:
us[alternatecodepage]
    Queries value:
                                                          HKCU\control panel\desktop[preferreduilanguages]
                                                          HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
    Oueries value:
    Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [prefer external manifest]
    Oueries value:
                                                          HKLM\system\currentcontrolset\control\nls\sorting\versions[]
                                                          HKCU\software\microsoft\windows
    Queries value:
nt\currentversion\appcompatflags[showdebuginfo]
    Queries value:
                                                          HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
    Queries value:
                                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
                                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
    Queries value:
options\dllnxoptions[fec00c2e3361c5caf7382f9ea1a7442f.exe]
                                                          HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\gre_initialize[disablemetafiles]
                                                          HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows
    Queries value:
nt\currentversion\compatibility32[fec00c2e3361c5caf7382f9ea1a7442f]
                                                          HKLM\software\wow6432node\microsoft\windows
    Oueries value:
nt\currentversion\windows[loadappinit_dlls]
                                                          HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
    Oueries value:
    Queries value:
                                                          HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
    Queries value:
                                                          HKLM\software\microsoft\ole[pageallocatorusesystemheap]
    Queries value:
                                                          HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
    Queries value:
                                                          HKLM\software\microsoft\ole[aggressivemtatesting]
                                                          HKLM\software\microsoft\sqmclient\windows[ceipenable]
    Oueries value:
    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]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
    Queries value:
                                                          HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
    Oueries value:
                                                          HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
    Queries value:
                                                          Oueries value:
                                                          HKLM\svstem\currentcontrolset\control\nls\sorting\ids[en-us]
    Queries value:
                                                          HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
                                                          HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Oueries value:
08002b30309d}\shellfolder[attributes]
    Queries value:
                                                          HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[callforattributes]
                                                          Oueries value:
08002b30309d}\shellfolder[restrictedattributes]
                                                          HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Oueries value:
08002b30309d}\shellfolder[foldervalueflags]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}]
                                                          HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Oueries value:
08002b30309d}\inprocserver32[]
    Oueries value:
```

```
11e3-be65-806e6f6e6963}[data]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-}
11e3-be65-806e6f6e6963}[generation]
 Oueries value:
                       HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
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]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
 Oueries value:
                       HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
 Queries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current \lor explorer \setminus advanced [mapnet drvbtn]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
                       HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
 Oueries value:
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
 Queries value:
Queries value:
                       HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-
97a27216f98a}\inprocserver32[]
                       HKCR\directory[docobject]
 Queries value:
                       HKCR\folder[docobject]
 Oueries value:
 Queries value:
                       HKCR\allfilesystemobjects[docobject]
 Queries value:
                       HKCR\directory[browseinplace]
 Oueries value:
                       HKCR\folder[browseinplace]
 Queries value:
                       HKCR\allfilesystemobjects[browseinplace]
 Oueries 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]
                       HKCR\allfilesystemobjects[nevershowext]
 Queries value:
                       HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-
 Oueries value:
a6bb2164fbd0}\inprocserver32[]
 Queries value:
                       HKLM\software\microsoft\com3[com+enabled]
                       HKCR \ wow 6432 node \ clsid \ \{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\}[]
 Queries value:
                       HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
 Oueries value:
b8dc300d9f9d}\inprocserver32[inprocserver32]
 Queries value:
                       HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[]
 Oueries value:
                       HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[threadingmodel]
                       HKLM\software\microsoft\ole[maxsxshashcount]
 Oueries value:
 Queries value:
db2c-424c-b029-7fe99a87c641}[category]
 Queries value:
db2c-424c-b029-7fe99a87c641}[name]
 Oueries value:
```

Queries value:

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

Oueries value

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

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma[]{\colorer.pdf} \end{subarrange} Abstraction \colorer. The properties of the pr$

Oueries value:

Queries value:

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

Oueries value:

 $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma\folderdescriptions\gamma\folderdescriptions\gamma\gamma\gamma\folderdescriptions\gamma\gam$

Oueries value:

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

Queries value:

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

Queries value

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

Queries value:

 $\label{local-equ$

Queries value:

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

Oueries value:

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value

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

Queries value:

 $\label{lem:hkcu} \verb+KKCU\+software\+microsoft\+windows\+currentversion\+explorer\+user\ shell$

folders[desktop]

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\f(1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}\currentversion\explorer\folder descriptions\f(1b3ea5dc-b587-4786-b4ef-bd1dc332aeae)\currentversion\explorer\folder\currentversion\explorer$

Queries value:

Queries value:

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

Oueries value:

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

Queries value:

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

Queries 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:

 $\label{thm:local-continuous} HKLM \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} wow 6432 node \end{tabular} microsoft \end{tabular} windows \end{tabular} \begin{tabular}{ll} HKLM \e$

b587-4786-b4ef-bd1dc332aeae}[icon]

Oueries value:

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

Queries value:

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

Oueries value

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value

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

Queries value:

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

Oueries value:

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

Queries value:

Oueries value

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

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

 $\label{lem:hklmsoftwarewow6432} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \folds \fol$

Queries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\ [localized name]$

Queries value

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folds 65f9-4cf6-a03a-e3ef65729f3d \cite{licon} \end{substitute}$

Queries value:

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

Queries value:

Queries value:

 $\label{local-hklm} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[streamresourcetype]$

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folds 65f9-4cf6-a03a-e3ef65729f3d \cite{lem:hklmsoftware} \cite{lem:hklmsoftware} \end{substitute} folds \cite{lem:hklmsoftware} \cite{lem:hklms$

Oueries value:

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

Oueries value

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

Ougries value

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

Queries value:

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

folders[appdata]

Queries value:

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

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

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value

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

Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder 6262-4760-9 afe-ea 3317 b 67173 \folder \$

Oueries value:

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

Queries value:

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

Queries value

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value

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

 $\label{lem:profile} Queries \ value: $$HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001[profileimagepath]$

Queries value: HKLM\software\wow6432node\microsoft\windows\windows error

reporting\wmr[disable]

 $\label{lem:queries} Queries \ value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath] \\ HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath] \\$

Queries value:

 $\label{lem:hccu} HKCU software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\mountpoints2| cpc \verb|\currentversion| explorer explor$

Queries value:

 $\label{lem:hcu} HKCU software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ \{d5291c63-7c88-11e3-be65-806e6f6e6963\} \cite{Absolution} \end{substitute}$

Oueries value:

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

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

options\dllnxoptions[system.dll]

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

options\dllnxoptions[nsexec.dll]

Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll]

Sets/Creates value:

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\mozillamaintenanceservice[displayname]
Sets/Creates value:

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\mozillamaintenanceservice[uninstallstring]
Sets/Creates value:

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\mozillamaintenanceservice[displayicon]
Sets/Creates value:

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\mozillamaintenanceservice[displayversion]
 Sets/Creates value:

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\mozillamaintenanceservice[publisher] Sets/Creates value:

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\mozillamaintenanceservice[comments]
Sets/Creates value:

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\mozillamaintenanceservice[nomodify]
Sets/Creates value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Wow 6432 node \label{lem:hklm} windows \label{lem:hklm} \label{lem:hklm} LM \label{lem:hklm} Wow 6432 node \label{lem:hklm} William \label{lem:hklm} Wow 6432 node \label{lem:hkklm} Wow 6432 no$

Sets/Creates value: HKLM\software\mozilla\maintenanceservice[attempted]
Sets/Creates value: HKLM\software\mozilla\maintenanceservice[installed]