Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 31, Task ID: 121

Task ID: 121 Risk Level: 4

Date Processed: 2016-04-28 12:50:18 (UTC)

Processing Time: 61.08 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

File System Events

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

Creates: C:\Users\Admin\AppData\Local\Temp\nsnA9D7.tmp

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

Opens: C:\Windows

Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\Sys\WO\W64

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

Opens: C:\Windows\Temp\bd9521b80b08a3c77a5f60c04f2adfe0.exe

 Opens:
 C:\Windows\SysWOW64\ntd11.dl1

 Opens:
 C:\Windows\SysWOW64\kernel32.dl1

 Opens:
 C:\Windows\SysWOW64\kernelBase.dl1

 Opens:
 C:\Windows\apppatch\sysmain.sdb

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

controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954

 $Opens: C: \windows \winsxs \x 86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954 \comctl32.dll$

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

C:\Windows\SysWOW64\cryptbase.dll Opens: Opens: C:\Windows\SysWOW64\sspicli.dll Opens: C:\Windows\SysWOW64\rpcrt4.dll C:\Windows\SysWOW64\shlwapi.dll Opens: C:\Windows\SysWOW64\shell32.dll Opens: C:\Windows\SysWOW64\advapi32.dll Opens: Opens: C:\Windows\SysWOW64\ole32.dll Opens: C:\Windows\SysWOW64\imm32.dll Opens: C:\Windows\SysWOW64\msctf.dll C:\Windows\SysWOW64\oleaut32.dll Opens: C:\Windows\SysWOW64\uxtheme.dll Opens: Opens: C:\Windows\SysWOW64\shfolder.dll

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

C:\Windows\SysWOW64\SHCore.dll

Opens: C:\

Opens:

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.ver0x00000000000000e.db

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

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

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

 Opens:
 C:\Windows\SysWOW64\cfgmgr32.dll

Opens: C:\Windows\SysWOW64\CTgmgr32.dl1
Opens: C:\Windows\SysWOW64\devobj.dl1
Opens: C:\Windows\SysWOW64\setupapi.dl1
Opens: C:\Users\Admin\AppData\Local\Temp\nsnA9D7.tmp

Opens: C:\Windows\SysWOW64\riched20.dll
Opens: C:\Windows\SysWOW64\lusp10.dll
Opens: C:\Windows\SysWOW64\lusp1331.dll
Opens: C:\Windows\Fonts\tahoma.ttf
Opens: C:\Windows\SysWOW64\dwmapi.dll

Opens: C:\Program Files (x86)

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

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

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

controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985

Opens: C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll

Opens: C:\Windows\WindowsShell.Manifest

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\nsnA9D7.tmp

Windows Registry Events

Opens key: HKLM\software\microsoft\wow64
Opens key: HKLM\system\currentcontrol\safeboot\option
Opens key: HKLM\system\currentcontrol\set\control\srp\gp\dll

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\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\language
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete

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

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

Opens key: HKCU\

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

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

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

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

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

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

 $Opens \ key: \\ HKLM \ software \ microsoft \ windows \\ nt \ current version \ app compatflags \ disable 8 and 16 bit mitigation \\$

Opens key:

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side \ as sembly storage roots$

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

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

execution options

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

options\dllnxoptions

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

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

nt\currentversion\compatibility32
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime

compatibility

Opens key: HKLM\

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

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

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

Opens key:

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

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

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

Opens key: HKLM\software\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

 $\label{lem:hklm} \verb+Kklm \+ software \+ microsoft \+ windows \+ current version \+ policies \+ explorer$ Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer Opens key:

Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids

Opens kev:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ bd9521b80b08a3c77a5f60c04f2adfe0.exe$

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

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

08002b30309d}\shellfolder

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \clsid \closer{lem:hkcu} \end{tabular} $$ -20d04fe0-explorer \clsid \closer{lem:hkcu} \end{tabular} $$ -20d04fe0-explorer \clsid \closer{lem:hkcu} \end{tabular} $$ -20d04fe0-explorer \clsid \closer{lem:hkcu} \closer{l$ Opens key:

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

Opens key:

a2d8-08002b30309d}\shellfolder

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

Opens key:

 $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version\\| policies\\| none num between the content of the co$

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

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

08002b30309d}\inprocserver32

Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2\ cpc \ volume \ \{d5291c64-7c88-4c40\} \ description \ de$

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}

HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-Opens key: 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 HKCU\software\microsoft\windows\currentversion\explorer\ Opens key:

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 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

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

Opens key: HKCR\allfilesystemobjects\docobject

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

HKCR\directory\browseinplace

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

Opens key: HKCR\folder\browseinplace

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

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

Opens key: HKCR\directory\clsid

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

Opens kev: HKCR\folder\clsid

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

Opens key: HKCR\allfilesystemobjects\clsid

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

a6bb2164fbd0}\inprocserver32

Opens key: HKLM\software\microsoft\com3

Opens key: HKLM\software\microsoft\windowsruntime\clsid

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

```
b8dc300d9f9d}
```

Opens kev: HKCR\activatableclasses\clsid

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

b8dc300d9f9d}

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

b8dc300d9f9d}\treatas

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler

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

b8dc300d9f9d}\inprochandler

Opens key:

Opens key:

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

Opens key:

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

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

Opens key:

 $\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \session in folders \end{tabular}$

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

folders

Opens key:

Opens key:

Opens key:

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

Opens key:

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

Opens key:

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

Opens key

 $\label{thm:local-prop} $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}}$

Opens key:

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

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

nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001

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

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

94f2-00a0c91efb8b}

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

94f2-00a0c91efb8b}\properties

Opens key:

 $HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ \{d5291c63-7c88-11e3-be65-806e6f6e6963\} \label{eq:hkcu}$

Opens key: HKLM\software\wow6432node\osm

Opens key: HKLM\system\currentcontrolset\control\nls\locale

Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
Opens key: HKLM\system\currentcontrolset\control\nls\language groups

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ ctf \ compatibility \ bd9521b80b08a3c77a5f60c04f2adfe0.exe$

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

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

Opens key: HKLM\software\microsoft\windows

 $nt\current version\label{language} age pack\datastore_v1.0$

Opens key: HKLM\software\microsoft\windows

 $\verb|nt/currentversion/languagepack/surrogatefallback| \\$

HKLM\software\microsoft\windows Opens key: nt\currentversion\languagepack\surrogatefallback\ms shell dlg 2 Opens key: HKLM\software\wow6432node\policies Opens key: HKCU\software\policies Opens key: HKCU\software Opens key: HKLM\software\wow6432node Opens key: HKCU\software\policies\microsoft\windows\currentversion\explorer\autocomplete HKCU\software\microsoft\windows\currentversion\explorer\autocomplete Opens kev: Opens key: HKLM\software\policies\microsoft\windows\currentversion\explorer\autocomplete Opens kev: Opens key: 00c04fd7d062} Opens key: HKCR\activatableclasses\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062} Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062} HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\treatas Opens key: $HKCR \setminus wow 6432 \\ node \\ clsid \\ \{00bb2765-6a77-11d0-a535-00c04fd7d062\} \\ \setminus treat \\ as$ Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32 HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-Opens key: 00c04fd7d062}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-Opens key: 00c04fd7d062}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\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 kev: 00aa005b43833 Opens key: Opens key: 00aa005b4383} Opens key: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383} Opens key: 00aa005b4383}\treatas $HKCR \setminus wow6432 node \\ clsid \setminus \{03c036f1-a186-11d0-824a-00aa005b4383\} \setminus treatas$ Opens key: Opens key: 00aa005b4383}\inprocserver32

HKLM\software\microsoft\windowsruntime\clsid\{03c036f1-a186-11d0-824a-

 $HKCR \ activatable classes \ \ \ \{03c036f1-a186-11d0-824a-00aa005b4383\}$ HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-

HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-

HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-

Opens key: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-

00aa005b4383}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-

00aa005b4383}\inprochandler32

HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-Opens key:

00aa005b4383}\inprochandler32

HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-Opens key:

00aa005b4383}\inprochandler

Opens key: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-

00aa005b4383}\inprochandler

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}

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

00c04fd7d062}

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

00c04fd7d062}\treatas

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

00c04fd7d062}\inprocserver32

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

00c04fd7d062}\inprocserver32

HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-Opens kev:

00c04fd7d062}\inprochandler32

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

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:

Opens key:

b61bb7cdd997}

Opens key: HKCR\activatableclasses\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}

HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-Opens key:

b61bb7cdd997}

Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997} Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-

b61bb7cdd997}\treatas

Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-Opens key:

b61bb7cdd997}\inprocserver32

HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-Opens key:

b61bb7cdd997}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-

b61bb7cdd997}\inprochandler32

HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-Opens key:

b61bb7cdd997}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-

b61bb7cdd997}\inprochandler

Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-

b61bb7cdd997}\inprochandler

 $HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| rpc \verb|\extensions||$ Opens key:

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

Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername

Opens key: HKLM\system\setup

 $\label{lem:hklm} \mbox{ HKLM\software\wow6432} node\policies\mbox{\swindows nt\rpc}$ Opens key:

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

Oueries value:

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

Queries value:

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

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

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

us[alternatecodepage]

Queries value: HKCU\control panel\desktop[preferreduilanguages]

HKCU\control panel\desktop\muicached[machinepreferreduilanguages] Queries value:

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]

 $HKLM \verb|\system| current controlset| control \verb|\nls| sorting| versions[]$ Oueries value:

HKCU\software\microsoft\windows Oueries 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]

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

options\dllnxoptions[bd9521b80b08a3c77a5f60c04f2adfe0.exe] HKLM\software\microsoft\windows Queries value: nt\currentversion\gre_initialize[disablemetafiles]

Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[bd9521b80b08a3c77a5f60c04f2adfe0] Oueries value: HKLM\software\wow6432node\microsoft\windows

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] Oueries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]

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

Queries value:

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

Queries value:

HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin] Oueries value:

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

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ policies \ explorer [no set folders]$

Queries value:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:local_hammon} software \end{tabular} in the internetion \end{tabular} and \begin{tabular}{ll} help the internetion \end{tabular} and \begin{tabular$

Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us] HKLM\svstem\currentcontrolset\control\nls\extendedlocale[en-us] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]

Oueries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us] Oueries 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-

08002b30309d}\shellfolder[attributes]

```
HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
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[foldervalueflags]
   Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{20d04fe0-3aea-1069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8
08002b30309d}1
                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\inprocserver32[]
   Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c64-7c88-4cq24, d54291c64-7c88-4cq24, d54291c644-7c88-4cq24, d54291c64-7c88-4cq24, d54291c64-7c88-4cq2406-7c86
11e3-be65-806e6f6e6963}[data]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-
11e3-be65-806e6f6e6963}[generation]
   Queries value:
                                                    HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
   Queries value:
                                                    HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
   Oueries value:
                                                    \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{linear} hidden \cite{linear} \end{tabular}
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
   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]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
                                                    HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
   Queries 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\currentversion\explorer\advanced[autocheckselect]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showstatusbar]
   Queries value:
                                                    HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-
97a27216f98a}\inprocserver32[]
                                                    HKCR\directory[docobject]
   Queries value:
   Oueries value:
                                                    HKCR\folder[docobject]
   Queries value:
                                                    HKCR\allfilesystemobjects[docobject]
   Queries value:
                                                    HKCR\directory[browseinplace]
   Queries value:
                                                    HKCR\folder[browseinplace]
                                                    HKCR\allfilesystemobjects[browseinplace]
   Oueries value:
                                                    HKCR\directory[isshortcut]
   Oueries value:
   Queries value:
                                                    HKCR\folder[isshortcut]
   Queries value:
                                                    HKCR\allfilesystemobjects[isshortcut]
   Queries value:
                                                    HKCR\directory[alwaysshowext]
   Queries value:
                                                    HKCR\directory[nevershowext]
   Oueries value:
                                                    HKCR\folder[nevershowext]
   Queries value:
                                                    HKCR\allfilesystemobjects[nevershowext]
                                                    HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-
   Oueries value:
a6bb2164fbd0}\inprocserver32[]
                                                    HKLM\software\microsoft\com3[com+enabled]
   Queries value:
                                                    HKCR \ wow 6432 node \ clsid \ \{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\}[]
   Queries value:
```

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

Queries value:

b8dc300d9f9d}\inprocserver32[inprocserver32]

Oueries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprocserver32[]

HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Queries value:

b8dc300d9f9d}\inprocserver32[threadingmodel]

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

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

Queries value:

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

Oueries value:

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

Oueries value:

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

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

Queries value:

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

Oueries value:

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

Queries value:

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

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

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

Queries value:

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

folders[desktop]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[category]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b264, 1b3ea5dc-b264, 1$ b587-4786-b4ef-bd1dc332aeae}[name]

Oueries value:

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

b587-4786-b4ef-bd1dc332aeae}[description]

b587-4786-b4ef-bd1dc332aeae}[relativepath]

Oueries value:

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

Queries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[infotip]

Queries value:

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

Oueries value:

Oueries value:

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

Oueries value:

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

Oueries value

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value

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

Oueries value:

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

Oueries value:

Queries value:

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

Oueries value

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

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

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

Queries value:

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

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 \mbox{$3eb685db-65f9-4cf6-a03a-e3ef65729f3d} [parentfolder]$

Queries value:

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

Queries value

 $\label{lem:hklm} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \eqref 6569-4cf6-a03a-e3ef65729f3d \cite{lem:hklm} \eqref folder \descriptions \eqref \descriptions \eqref folder \eqref folder \descriptions \eqref folder \eqref folder \eqref folder \descriptions \eqref folder \eqref fo$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432} HKLM \software \wow6432 node \mbox{$3eb685db-65f9-4cf6-a03a-e3ef65729f3d} [stream resource]$

Oueries value:

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

Oueries value

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

Queries value:

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

Oueries value

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

Queries value:

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

Oueries value:

 $\label{thm:local-prop} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \calebox{3eb685db-65f9-4cf6-a03a-e3ef65729f3d} \cite{thm:local-prop} \cite{t$

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

folders[appdata]

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1}{2} each \footnote{1}{2} each \footnote{2}{2} each \footnote{2} each \footnote{2}{2} each \footnote{2} each \footnote{2}{2} each \footnote{2} each \footnote{2}{2} each \footnote{2} each \footnote{2} each \footnote{2} each \footnote{2}{2} each \footnote{2} each \footnot$

Queries value:

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

Oueries value:

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

 $H\dot{L}M\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresource]

Queries value

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

Queries value:

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

Oueries value:

 $\label{local-prop} \begin{tabular}{ll} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions$

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1}{2} e6c858f-0e22-4760-9 af e-ea3317 b67173 \[publish expanded path]$

Queries value:

```
0e22-4760-9afe-ea3317b67173}[attributes]
   Queries value:
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}[foldertypeid]
0e22-4760-9afe-ea3317b67173}[initfolderhandler]
                                               Oueries value:
1923240461-1905901954-2556564120-1001[profileimagepath]
                                               HKLM\software\wow6432node\microsoft\windows\windows error
   Oueries value:
reporting\wmr[disable]
   Queries value:
                                               HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
                                               HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
   Queries value:
   Queries value:
11e3-be65-806e6f6e6963}[data]
   Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c63-7c88-4c64, d5291c63-7c88-4c64, d5291c64, d5291c64, d5291c64, d5291c64, d5291c64, d5291c64, d5291c64, d5291c644, d5291c64, d5291c64, d5291c64, d5291c64, d5291c64, d5291c64, 
11e3-be65-806e6f6e6963}[generation]
   Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]
                                               HKLM\system\currentcontrolset\control\nls\locale[00000409]
   Queries value:
   Queries value:
                                               HKLM\system\currentcontrolset\control\nls\language groups[1]
   Oueries value:
                                               HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
                                               HKLM\software\microsoft\windows
   Oueries 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]
   Queries value:
                                               HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane2]|
                                               HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback[plane3]
   Queries value:
                                               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
   Queries value:
                                               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
   Oueries value:
                                               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
                                               HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback[plane7]
   Oueries value:
                                               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
                                               HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback[plane9]
   Queries value:
                                               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
   Oueries value:
                                               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
                                               HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane12]
                                               HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback[plane13]
   Queries value:
                                               HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane14]|
                                               HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback[plane15]
   Oueries value:
                                               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]
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
   Queries value:
                                               HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}[]
   Oueries value:
                                               HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
                                               HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
   Queries value:
00c04fd7d062}\inprocserver32[1
   Queries value:
                                               HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
                                               HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}[]
   Queries value:
   Queries value:
                                               HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
```

00aa005b4383}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-

00aa005b4383}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-

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]

Queries value: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-

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[]
Queries value: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}[]

Queries value: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-

b61bb7cdd997}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-

b61bb7cdd997}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-

b61bb7cdd997}\inprocserver32[threadingmodel]

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

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

Queries value:

Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup[systemsetupinprogress]
Queries value: HKLM\software\microsoft\rpc[idletimerwindow]
Queries value: HKCU\control panel\desktop[smoothscroll]

Queries value:

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

Oueries value:

Queries value:

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

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[acclistviewv6]

Queries value:

Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe

ui]