Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 150, Task ID: 598

Task ID: 598

Risk Level: 4

Date Processed: 2016-04-28 13:03:18 (UTC)

Processing Time: 2.31 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\e8663e22fd4ed76c67608ee879788437.exe"

Sample ID: 150 Type: basic Owner: admin

Label: e8663e22fd4ed76c67608ee879788437

Date Added: 2016-04-28 12:45:05 (UTC)

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

MD5: e8663e22fd4ed76c67608ee879788437

SHA256: 76854ea46800be903eed511def10040917475c931eec0e335f0c030f6ecf3272

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\e8663e22fd4ed76c67608ee879788437.exe

["C:\windows\temp\e8663e22fd4ed76c67608ee879788437.exe"]

Terminates process: C:\Windows\Temp\e8663e22fd4ed76c67608ee879788437.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\nsx6915.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\nsn6926.tmp

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

Creates: C:\Users\Admin\AppData\Local
Creates: C:\Users\Admin\AppData\Local\Temp
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\nsn6926.tmp\nsExec.dll

Creates: C:\Program Files (x86)\Mozilla Maintenance Service\Uninstall.exe
Opens: C:\Windows\Prefetch\E8663E22FD4ED76C67608EE879788-F232FE32.pf

Opens: C:\Windows

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

Opens: C:\Windows\SysWOW64
Opens: C:\Windows\SysWOW64

Opens: C:\Windows\SysW0W64\apphelp.dll

Opens: C:\Windows\Temp\e8663e22fd4ed76c67608ee879788437.exe
Opens: C:\Windows\SysWOW64\ntdl1.dl1

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\version.dll
Opens: C:\Windows\SysWOW64\combase.dll
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\Windows\SysWOW64\gdi32.dll
Opens: C:\Windows\SysWOW64\user32.dll
Opens: C:\Windows\SysWOW64\user32.dll

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:

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 C:\Windows\SysWOW64\desktop.ini Opens: C:\Users\Admin\Desktop\desktop.ini Opens: Opens: C:\Windows\SysWOW64\profapi.dll

Opens: C:\Users\Admin\AppData\Local\Temp\nsx6915.tmp

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

Opens: C:\Users\Admin\AppData\Local\Temp\nsn6926.tmp

Opens: C:\Users\Admin\AppData\Local\Temp\nsn6926.tmp\System.dll Opens: C:\Program Files (x86)\Mozilla Maintenance Service

Opens: C:\Windows\Temp

C:\Users\Admin\AppData\Local\Temp\nsn6926.tmp\nsExec.dll Opens:

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

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

Opens: C:\Users\Admin

C:\Users Opens:

Writes to: C:\Users\Admin\AppData\Local\Temp\nsn6926.tmp\System.dll Writes to: C:\Users\Admin\AppData\Local\Temp\nsn6926.tmp\nsExec.dll Writes to: C:\Program Files (x86)\Mozilla Maintenance Service\Uninstall.exe

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

C:\Windows\Temp\e8663e22fd4ed76c67608ee879788437.exe Reads from: Deletes: C:\Users\Admin\AppData\Local\Temp\nsx6915.tmp C:\Users\Admin\AppData\Local\Temp\nsn6926.tmp Deletes:

Deletes: C:\Users\Admin\AppData\Local\Temp\nsn6926.tmp\nsExec.dll Deletes: C:\Users\Admin\AppData\Local\Temp\nsn6926.tmp\System.dll

Windows Registry Events

Creates key:

HKLM\software\mozilla\maintenanceservice Creates key:

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

Deletes value: $HKLM \setminus software \setminus mozilla \setminus maintenance service [ffprefetch disabled] \\$

Opens key: HKLM\software\microsoft\wow64

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

HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers

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

HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings

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

Opens key:

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 kev: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\disable8and16bitmitigation

Opens key:

Opens kev: 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

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

nt\currentversion\compatibility32

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

compatibility

Opens key:

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

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\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: $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \label{lem:hkcu} \\ direct manipulation$

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

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ 8663e22fd 4ed 76c6 7608ee 879788437.exe$

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

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:

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

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2\ cpc \ volume \ \{d5291c64-7c88-4c64-7c8$

11e3-be65-806e6f6e6963}\

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

Opens key: HKCR\drive\shellex\folderextensions

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

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: $HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-407034-ac3f-4070$

97a27216f98a}\inprocserver32

HKCU\software\classes\directory Opens key:

Opens key: HKCR\directory

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

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

Opens key: HKCR\folder

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

Opens key: HKCR\folder\shellex\iconhandler

HKCU\software\classes\allfilesystemobjects Opens key:

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
                                                                             HKCR\folder\browseinplace
     Opens key:
     Opens key:
                                                                             HKCU\software\classes\allfilesystemobjects\browseinplace
     Opens key:
                                                                             HKCR\allfilesystemobjects\browseinplace
     Opens kev:
                                                                             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-bd2c-
 a6bb2164fbd0}\inprocserver32
     Opens key:
                                                                             HKLM\software\microsoft\com3
     Opens key:
                                                                             HKLM\software\microsoft\windowsruntime\clsid
     Opens key:
                                                                             b8dc300d9f9d}
     Opens key:
                                                                             HKCR\activatableclasses\clsid
     Opens key:
                                                                             HKCR\activatableclasses\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
     Opens kev:
                                                                             HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}
     Opens key:
                                                                             HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
     Opens key:
                                                                             HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\treatas
     Opens key:
                                                                             HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas
                                                                             HKCU \setminus software \setminus classes \setminus wow 6432 node \setminus clsid \setminus \{1f486a52 - 3cb1 - 48fd - 8f50 -
     Opens key:
b8dc300d9f9d}\inprocserver32
     Opens key:
                                                                             HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32
                                                                             HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
     Opens key:
b8dc300d9f9d}\inprochandler32
     Opens key:
                                                                             HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler32
     Opens kev:
                                                                             HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler
     Opens key:
                                                                             HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler
     Opens kev:
Opens key:
db2c-424c-b029-7fe99a87c641}
     Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ f
db2c-424c-b029-7fe99a87c641}\propertybag
                                                                             HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
     Opens key:
     Opens key:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in folders
     Opens key:
                                                                             HKCU\software\microsoft\windows\currentversion\explorer\user shell
 folders
     Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings
     Opens kev:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-baseline \ and \ baseline \ and \ and \ baseline \ and \ and \ baseline \ and \ and \ baseline \ and \ baseline \ and \ and
b587-4786-b4ef-bd1dc332aeae}
     Opens key:
b587-4786-b4ef-bd1dc332aeae}\propertybag
     Opens key:
65f9-4cf6-a03a-e3ef65729f3d}
HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685db-16422 \\ node \setminus \{3eb68
65f9-4cf6-a03a-e3ef65729f3d}\propertybag
     Opens key:
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 key:
                                                                             \label{lem:hklmsoftware} HKLM \software \mbox{\sc nt} \c urrent version \profile list \sc -1-5-21-1000 \end{\sc nt} .
 1923240461-1905901954-2556564120-1001
```

HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr

Opens key:

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

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

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

 $HKLM \setminus system \setminus current control \setminus device classes \setminus \{53f5630d-b6bf-11d0-b6b$ Opens key:

94f2-00a0c91efb8b}

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

94f2-00a0c91efb8b}\properties

HKLM\software\wow6432node\mozilla\maintenanceservice Opens key:

Opens key:

 $HKCU \setminus software \setminus icrosoft \setminus ic$

11e3-be65-806e6f6e6963}\

Opens kev: HKLM\software\mozilla\maintenanceservice

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

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

Queries 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]

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

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

us[alternatecodepage]

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

 $\label{lem:hkcu} \verb+KCU+ control panel+ desktop+ muicached[machine preferred uil anguages]+ \\$ Queries value:

Oueries value:

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

HKCU\software\microsoft\windows Oueries value:

nt\currentversion\appcompatflags[showdebuginfo]

Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Oueries value:

options\dllnxoptions[usefilter]

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

options\dllnxoptions[e8663e22fd4ed76c67608ee879788437.exe] HKLM\software\microsoft\windows Oueries value:

nt\currentversion\gre_initialize[disablemetafiles]

HKLM\software\wow6432node\microsoft\windows Queries value: $\verb|nt\currentversion\compatibility32[e8663e22fd4ed76c67608ee879788437]|$ HKLM\software\wow6432node\microsoft\windows Queries value:

nt\currentversion\windows[loadappinit_dlls]

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

Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy] HKLM\software\microsoft\ole[pageallocatorusesystemheap] Oueries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Oueries value:

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

Queries value:

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

Oueries value:

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

HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel] Queries value:

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

Oueries value:

HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon] HKLM\system\currentcontrolset\control\nls\customlocale[en-us] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us] Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]

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

Oueries 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]

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

08002b30309d}\shellfolder[restrictedattributes]

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

08002b30309d}\shellfolder[foldervalueflags]

Oueries value:

HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-

08002b30309d}1

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

08002b30309d}\inprocserver32[]

Oueries value:

11e3-be65-806e6f6e6963}[data]

Queries value:

```
11e3-be65-806e6f6e6963}[generation]
 Oueries value:
                      HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
 Queries value:
Oueries value:
                      HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
                      HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
                      HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
 Queries value:
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showstatusbar]
                      HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-
 Oueries value:
97a27216f98a}\inprocserver32[]
 Queries value:
                      HKCR\directory[docobject]
 Queries value:
                      HKCR\folder[docobject]
 Queries value:
                      HKCR\allfilesystemobjects[docobject]
                      HKCR\directory[browseinplace]
 Oueries value:
 Queries value:
                      HKCR\folder[browseinplace]
                      HKCR\allfilesystemobjects[browseinplace]
 Oueries value:
 Queries value:
                      HKCR\directory[isshortcut]
 Queries value:
                      HKCR\folder[isshortcut]
 Oueries value:
                      HKCR\allfilesystemobjects[isshortcut]
 Queries value:
                      HKCR\directory[alwaysshowext]
                      HKCR\directory[nevershowext]
 Oueries value:
 Queries value:
                      HKCR\folder[nevershowext]
 Queries value:
                      HKCR\allfilesystemobjects[nevershowext]
                      HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-
 Queries 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-
 Oueries value:
b8dc300d9f9d}\inprocserver32[inprocserver32]
 Queries value:
                      HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[]
                      HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
 Oueries value:
b8dc300d9f9d}\inprocserver32[threadingmodel]
                     HKLM\software\microsoft\ole[maxsxshashcount]
 Queries value:
 Queries value:
db2c-424c-b029-7fe99a87c641}[category]
 Oueries value:
db2c-424c-b029-7fe99a87c641}[name]
 Oueries value:
db2c-424c-b029-7fe99a87c641}[parentfolder]
```

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

Queries value:

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

Queries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[parsingname]

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value

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

Queries value:

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

Queries value:

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

folders[desktop]

Queries value:

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

Queries value:

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

Queries value:

Queries value

Queries value:

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

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

 $\label{thm:local-holes} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[streamresourcetype]$

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:

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

Oueries value:

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

Oueries value:

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

Queries value

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

Oueries 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:

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

Oueries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{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:

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

Oueries value:

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

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parsingname]

Oueries value

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

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

Oueries value:

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

Queries value

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

Queries value:

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

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries 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:

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

Queries value:

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

Queries value:

 $\label{lem:hklm} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \current \end{5e6c858f-0e22-4760-9afe-ea3317b67173} \ [roamable]$

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

Queries value:

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

Oueries value

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

Queries value:

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

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]

Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]

Queries 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:

 $HKCU \ software \ `microsoft \ `windows \ current version \ explorer \ `mountpoints2 \ cpc \ volume \ \{d5291c63-7c88-11e3-be65-806e6f6e6963\} \ [data]$

Queries value:

 $\label{lem:hcu} HKCU software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\mountpoints2| cpc \verb|\volume| {d5291c63-7c88-11e3-be65-806e6f6e6963} [generation]$

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

Sets/Creates value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ uninstall \ mozillama intenances ervice [display name] \\ Sets \ / Creates \ value:$

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:

 $\label{lem:hklmsoftware} HKLM software \noinder microsoft \noinder lambda in tenance service [publisher] Sets/Creates value:$

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

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

 $HKLM \label{lem:hklm} Which is a simple that the simple that$

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