Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 225, Task ID: 898

Task ID: 898

Risk Level: 4

Date Processed: 2016-04-28 13:12:20 (UTC)

Processing Time: 3.26 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\6d438b3e1ec4eca849107b093ce99dbc.exe"

Sample ID: 225 Type: basic Owner: admin

Label: 6d438b3e1ec4eca849107b093ce99dbc

Date Added: 2016-04-28 12:45:13 (UTC)

File Type: PE32:win32:gui File Size: 927416 bytes

MD5: 6d438b3e1ec4eca849107b093ce99dbc

SHA256: 9977dc742345ebc75d8914773e0af884e6ee16227f7acf9361fff7b681b971fc

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\6d438b3e1ec4eca849107b093ce99dbc.exe

["C:\windows\temp\6d438b3e1ec4eca849107b093ce99dbc.exe"]

Terminates process: C:\Windows\Temp\6d438b3e1ec4eca849107b093ce99dbc.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\nsj3A35.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\nse3AB3.tmp

Creates: C:\Users
Creates: C:\Users\Admin
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:\Users\Admin\AppData\Local\Temp\nse3AB3.tmp\System.dll
Creates: C:\Users\Admin\AppData\Local\Temp\nse3AB3.tmp\CityHash.dll
Opens: C:\Windows\Prefetch\6D438B3E1EC4ECA849107B093CE99-F2941E4F.pf

Opens: C:\Windows

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

Opens: C:\Windows\SysWOW64

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

Opens: C:\Windows\Temp\6d438b3e1ec4eca849107b093ce99dbc.exe

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

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

controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985

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

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

Opens: C:\Windows\syswOw64\cryptbase.dl
Opens: C:\Windows\SyswOW64\sspicli.dll
Opens: C:\Windows\SyswOW64\rpcrt4.dll
Opens: C:\Windows\SyswOW64\shlwapi.dll
Opens: C:\Windows\SyswOW64\shell32.dll
Opens: C:\Windows\SyswOW64\advapi32.dll

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

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

Opens: C:\

Opens: C:\Windows\Sys\WO\W64\clbcatq.dll
Opens: C:\Windows\Sys\WO\W64\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:\Users\Admin\AppData\Local\Temp\nsj3A35.tmp

Opens: C:\Windows\SysWOW64\cfgmgr32.dll
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\nse3AB3.tmp

Opens: C:\Users\Admin\AppData\Local\Temp\nse3AB3.tmp\System.dll

Opens: C:\Program Files (x86)

Opens: C:\Users\Admin\AppData\Local\Temp\nse3AB3.tmp\CityHash.dll

Opens: C:\windows\temp\distribution\

Opens: C:\Windows\Temp

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

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

Writes to: C:\Users\Admin\AppData\Local\Temp\nse3AB3.tmp\System.dll
Writes to: C:\Users\Admin\AppData\Local\Temp\nse3AB3.tmp\CityHash.dll

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

Reads from: C:\Windows\Temp\6d438b3e1ec4eca849107b093ce99dbc.exe
Deletes: C:\Users\Admin\AppData\Local\Temp\nsj3A35.tmp
Deletes: C:\Users\Admin\AppData\Local\Temp\nse3AB3.tmp

Deletes: C:\Users\Admin\AppData\Local\Temp\nse3AB3.tmp\CityHash.dll
Deletes: C:\Users\Admin\AppData\Local\Temp\nse3AB3.tmp\System.dll

Windows Registry Events

Creates key: HKLM\software\wow6432node\mozilla\thunderbird\taskbarids

Creates key: HKLM\software\wow6432node

Creates key: HKLM\software\wow6432node\mozilla

Creates key: HKLM\software\wow6432node\mozilla\thunderbird

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:

Opens key.

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\language
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages

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

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

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

Opens key: HKCU\

Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration

 $Opens~key: \\ HKLM\system\current control set\control\mui\settings\language configuration$

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

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

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

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

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

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

Opens key:

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

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

nt\currentversion\compatibility32

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

compatibility

Opens key:

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

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

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

Opens key:

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

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

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

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

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

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

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

Opens key:

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

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

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ 6d438b3e1ec4eca849107b093ce99dbc.exe$

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

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\clsid| {20d04fe0-properties of the context of the$ Opens key:

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

Opens kev:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-

a2d8-08002b30309d}\shellfolder

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

Opens key:

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

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

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

08002b30309d}\inprocserver32

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ \ explorer \ \ mountpoints 2 \ \ cpc \ \ \ volume$

Opens key:

11e3-be65-806e6f6e6963}\

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

Opens key: HKCR\drive\shellex\folderextensions

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

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

4442-804e-409d6c4515e9} 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 HKCU\software\microsoft\windows\currentversion\explorer Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\

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

Opens key: $HKCR\wow6432 node\clsid\{a07034fd-6caa-4954-ac3f-407034-ac3f-4070707-ac3f-40707-ac3f-40707-ac3f-40707-ac3f-40707-ac3f-40707-ac3f-40707-ac3f-40707-ac3f-40707-ac3$

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

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

Opens key: HKCR\folder\shellex\iconhandler

Opens key: HKCU\software\classes\allfilesystemobjects

Opens key: HKCR\allfilesystemobjects

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

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

Opens key: HKCR\directory\docobject

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

Opens key: HKCR\folder\docobiect

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

Opens key: HKCR\allfilesystemobjects\docobject

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

HKCR\directory\browseinplace Opens key:

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

b8dc300d9f9d}

Opens key: HKCR\activatableclasses\clsid

Opens key: HKCR\activatableclasses\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
Opens key: HKCU\software\classes\www6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}

b8dc300d9f9d}\treatas

 $\label{linear_control_openskey} Openskey: $$ HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas$$ Openskey: $$ HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas$$ Openskey: $$ HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas$$ Openskey: $$ HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas$$ Openskey: $$ HKCU\software\clsid\clsi$

b8dc300d9f9d}\inprocserver32

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

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

Opens key:

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

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

Opens key:

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

folders

Opens key:

Opens key

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

Opens key:

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

Opens key:

 $\label{local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \colored \folder \folde$

Opens key:

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

Opens key:

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

Opens key:

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

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\www6432node\microsoft\windows\windows error reporting\wmr
Opens key: HKLM\software\www6432node\microsoft\windows\currentversion\setup

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

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

94f2-00a0c91efb8b}

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

94f2-00a0c91efb8b}\properties

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints 2 \ cpc \ volume \ \{d5291c63-7c88-1c44, d5291c63-7c88-1c44, d52$

11e3-be65-806e6f6e6963}\

Opens key: HKLM\software\wow6432node\mozilla\thunderbird\taskbarids

Opens key: HKCU\software\mozilla\thunderbird\taskbarids

Opens key: HKLM\software

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

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

Oueries value:

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

Oueries value:

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

 $\label{lem:hklm} \verb+Kklm \ system \ \verb+current \ control \ \verb+mui \ \verb+uilanguages \ \verb+en-us[type]+ \\$ Queries value:

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

us[alternatecodepage]

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

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [prefer external manifest]$

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

Queries value: HKCU\software\microsoft\windows

nt\currentversion\appcompatflags[showdebuginfo]

HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution Oueries value:

options\dllnxoptions[usefilter]

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

options\dllnxoptions[6d438b3e1ec4eca849107b093ce99dbc.exe] Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]

Oueries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[6d438b3e1ec4eca849107b093ce99dbc] HKLM\software\wow6432node\microsoft\windows Oueries value:

nt\currentversion\windows[loadappinit_dlls]

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

Oueries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy] HKLM\software\microsoft\ole[pageallocatorusesystemheap] Queries value: ${\tt HKLM \setminus software \setminus microsoft \setminus ole[pageallocator system heap is private]}$ Queries value:

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

Oueries value:

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

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

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

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

HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[attributes]

Oueries value:

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

08002b30309d}\shellfolder[callforattributes] Oueries value:

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

08002b30309d}\shellfolder[restrictedattributes]

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

08002b30309d}\shellfolder[foldervalueflags]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\ \{20d04fe0-3aea-1069-a2d8-4064fe0-3aea-1069-a2d8-4064fe0-3aea-1069-a2d8-4064fe0-3aea-1069-a2d8-4064fe0-3aea-1069-a2d8-4064fe0-3aea-1069-a2d8-4064fe0-3aea-1069-a2d8-4064fe0-3aea-1069-a2d8-4064fe0-3aea-1069-a2d8-4064fe0-3aea-1069-a2d8-4064fe0-3aea-1069-a2d8-4064fe0-3aea-1069-a2d8-4064fe0-3aea-1069-a2d8-4064fe0-3aea-1069-a2d8-4064fe0-3aea-1069-a2d8-4064fe0-3aea-1069-a2d8-4064fe0-3aea-1069-a2d8-4064fe0-3aea-1069-a2d8-4064fe0-3aea-1069-a2d8-4064fe0-3aea-40$

08002b30309d}]

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

08002b30309d}\inprocserver32[]

Queries value:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints 2 \ cpc \ volume \ \{d5291c64-7c88-4c14, d5291c64-7c88-4c14, d5291c64-7c88-4c140, d5291c64-7c88-4c1464-7c88-4c140, d5291c64-7c88-4c140, d5291c64-7c88-4c140, d5291c6$

11e3-be65-806e6f6e6963}[data]

Oueries value:

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

11e3-be65-806e6f6e6963}[generation]

HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-Queries value:

409d6c4515e9}[drivemask]

Queries value:

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

Oueries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate]

```
Oueries value:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [nowebview]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
                                    HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
  Oueries value:
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
  Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced [show superhidden]
  Queries value:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \current version \explorer \advanced [separate process] \end{tabular}
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showstatusbar]
                                    HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-
  Queries value:
97a27216f98a}\inprocserver32[]
  Queries value:
                                    HKCR\directory[docobject]
  Queries value:
                                    HKCR\folder[docobject]
                                    HKCR\allfilesystemobjects[docobject]
  Oueries value:
                                    HKCR\directory[browseinplace]
  Oueries value:
  Oueries value:
                                    HKCR\folder[browseinplace]
  Queries value:
                                    HKCR\allfilesystemobjects[browseinplace]
  Queries value:
                                    HKCR\directory[isshortcut]
  Queries value:
                                    HKCR\folder[isshortcut]
  Oueries value:
                                    HKCR\allfilesystemobjects[isshortcut]
                                    HKCR\directory[alwaysshowext]
  Oueries value:
                                    HKCR\directory[nevershowext]
  Queries value:
  Oueries value:
                                    HKCR\folder[nevershowext]
  Queries value:
                                    HKCR\allfilesystemobjects[nevershowext]
  Queries value:
                                    HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-
a6bb2164fbd0}\inprocserver32[]
  Queries value:
                                    HKLM\software\microsoft\com3[com+enabled]
                                    HKCR \ wow 6432 node \ clsid \ \{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\}[]
  Oueries value:
  Queries value:
                                    HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[inprocserver32]
                                    HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
  Oueries value:
b8dc300d9f9d}\inprocserver32[]
                                    HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
  Oueries value:
b8dc300d9f9d}\inprocserver32[threadingmodel]
                                   HKLM\software\microsoft\ole[maxsxshashcount]
  Oueries value:
  Queries value:
db2c-424c-b029-7fe99a87c641}[category]
db2c-424c-b029-7fe99a87c641}[name]
  Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ f
db2c-424c-b029-7fe99a87c641}[parentfolder]
  Oueries value:
db2c-424c-b029-7fe99a87c641}[description]
  Oueries value:
db2c-424c-b029-7fe99a87c641}[relativepath]
```

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

Oueries value:

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

Queries value:

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\\folderdescriptions\\\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}[icon]$

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value

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

Queries value:

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

Oueries value:

Queries value:

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

Oueries value

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

folders[desktop]

Queries value:

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

Queries value

 $\label{thm:local-basis} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\f(1b3ea5dc-b587-4786-b4ef-bd1dc332 aeae)\cite{local-b587-4786-b4ef-bd1dc332}.$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

Oueries value:

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

Oueries value

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

Oueries 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:

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

Oueries value:

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

Queries 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:

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

Queries value:

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

Queries value:

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

Oueries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder descriptions\folder descriptions\folder description\folder descriptio$

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value

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

Queries value:

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

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432} HKLM \software \wow6432 node \windows \current version \explorer \folder descriptions \eqref 65f9-4cf6-a03a-e3ef65729f3d \solution{ Stream resource type of the property of$

Queries value

Queries value:

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

Oueries value:

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

folders[appdata]

Queries value:

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

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1.5} Ge6c858f-0e22-4760-9 af e-ea3317b67173 \cite{1.5} [name]$

Oueries value:

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

Oueries value:

 $\label{thm:local-prop} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \current \current$

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

Queries value:

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

Oueries value

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder description$

Queries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder type id]$

Queries value:

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

Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001[profileimagepath]

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

reporting\wmr[disable]

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

Queries value:

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

Queries value:

 $\label{lem:hkculsoftware} Hkculsoftware \end{d5291c63-7c88-11e3-be65-806e6f6e6963} [generation]$

Oueries value:

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

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

options\dllnxoptions[system.dll]

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

Sets/Creates value: HKLM\software\wow6432node\mozilla\thunderbird\taskbarids[c:\program

files (x86)\mozilla thunderbird]