Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 131, Task ID: 522

Task ID: 522

Risk Level: 4

Date Processed: 2016-04-28 13:01:23 (UTC)

Processing Time: 2.77 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\2a3d6128a1b210860531603f74a24c7f.exe"

Sample ID: 131
Type: basic
Owner: admin

Label: 2a3d6128a1b210860531603f74a24c7f

Date Added: 2016-04-28 12:45:03 (UTC)

File Type: PE32:win32:gui File Size: 620911 bytes

MD5: 2a3d6128a1b210860531603f74a24c7f

SHA256: cca1510e63a3ab7c4679ab5043dd4c3e0ba1dfcabc2e36c67edd3d46793a8134

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\2a3d6128a1b210860531603f74a24c7f.exe

["C:\windows\temp\2a3d6128a1b210860531603f74a24c7f.exe"]

Terminates process: C:\Windows\Temp\2a3d6128a1b210860531603f74a24c7f.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\nskAF36.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\nskAF37.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\nsaAF48.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\nsaAF48.tmp\nsHelper.dll
Opens: C:\Windows\Prefetch\2A3D6128A1B210860531603F74A24-4C63C17E.pf

Opens: C:\Windows

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

Opens: C:\Windows\SysWOW64

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

Opens: C:\Windows\Temp\2a3d6128a1b210860531603f74a24c7f.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

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

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\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:
Opens:
                        C:\Windows\SysWOW64\imm32.dll
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
```

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

Opens: C:\

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

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

C:\Users\Admin\AppData\Local\Temp\nskAF36.tmp Opens:

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\nsaAF48.tmp

Opens: C:\Users\Admin\AppData\Local\Temp\nsaAF48.tmp\nsHelper.dll

Opens: C:\Windows\SysWOW64\iertutil.dll C:\Windows\SysWOW64\wininet.dll Opens: Opens: C:\Windows\SysWOW64\urlmon.dll Opens: C:\Program Files (x86)\XingHaoLyrics\ C:\Program Files (x86)\LyricsPal\ Opens: C:\Users\Admin\AppData\Local Opens: Opens: C:\Users\Admin\AppData

Opens: C:\Users\Admin

Opens: C:\Users

Writes to: C:\Users\Admin\AppData\Local\Temp\nskAF37.tmp

Writes to: C:\Users\Admin\AppData\Local\Temp\nsaAF48.tmp\nsHelper.dll

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

C:\Windows\Temp\2a3d6128a1b210860531603f74a24c7f.exe Reads from: Reads from: C:\Users\Admin\AppData\Local\Temp\nskAF37.tmp Deletes: C:\Users\Admin\AppData\Local\Temp\nskAF36.tmp Deletes: C:\Users\Admin\AppData\Local\Temp\nsaAF48.tmp

Deletes:

Windows Registry Events

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 kev: 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:

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

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

HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots

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

Opens key: $\label{lem:hklm} \mbox{ HKLM\software\wow6432} node\mbox{ microsoft\windows nt\currentversion\simple} ille \mbox{ file} \mbox{ file} \mbox{ microsoft\windows nt\currentversion\simple} \mbox{ file} \mbox{ microsoft\windows nt\currentversion\simple} \mbox{ file} \mbox{ microsoft\windows nt\currentversion\simple} \mbox{ microsoft\windows nt\currentversion\simple} \mbox{ microsoft\windows nt\current\simple} \mbox{ microsoft\windows nt\current\simple} \mbox{ microsoft\simple} \mbox{ microsoft\s$

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

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:

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

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

Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKLM\system\currentcontrol\nls\extendedlocale

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

Opens key:

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus shell compatibility \setminus applications \setminus 2a3d6128a1b210860531603f74a24c7f. exercise the substitution of the substitution is a substitution of the substitu$

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

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

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

Opens key:

a2d8-08002b30309d}\shellfolder

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

Opens key:

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

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

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

08002b30309d}\inprocserver32

Opens key:

 $\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \end{tabular} \label{thm:linear}$

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c64-7c88-4c144, d5291c64-7c88-4c144, d5291c64-$

11e3-be65-806e6f6e6963}\

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

Opens key: HKCR\drive\shellex\folderextensions

 $Opens~key: \\ HKCU \ Software \ Classes \ drive \ Shellex \ folder extensions \ (fbeb8a05-beee-beed) \\ If the beautiful of the context of th$

4442-804e-409d6c4515e9} Opens key:

Opens key: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}

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\

 $Opens\ key: \\ HKCU \ software \ microsoft \ windows \ current version \ \ explorer \ \ advanced$

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

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

Opens key: HKCR\folder\shellex\iconhandler

Opens key: ${\tt HKCU \backslash software \backslash classes \backslash all filesystemobjects}$

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

 ${\tt Opens\,key:} \qquad \qquad {\tt HKCU\setminus software \setminus classes \setminus allfilesystemobjects \setminus browseinplace}$

```
Opens key:
                                                           HKCR\allfilesystemobjects\browseinplace
                                                           HKCU\software\classes\directory\clsid
   Opens key:
   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:
                                                           {\tt 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 kev:
                                                           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}
                                                           HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
   Opens kev:
b8dc300d9f9d}
   Opens key:
                                                           HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
   Opens key:
                                                           HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\treatas
                                                           HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas
   Opens key:
   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 kev:
b8dc300d9f9d}\inprochandler32
                                                           HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
   Opens kev:
b8dc300d9f9d}\inprochandler32
                                                           HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
   Opens key:
b8dc300d9f9d}\inprochandler
                                                           HKCR \setminus wow 6432 \\ node \\ \clsid \\ \cl
   Opens key:
b8dc300d9f9d}\inprochandler
```

Opens key:

Opens key:

db2c-424c-b029-7fe99a87c641}

Opens key:

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

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

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:

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dcb587-4786-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

0e22-4760-9afe-ea3317b67173}

Opens key:

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

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

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

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

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

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

94f2-00a0c91efb8b}

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

94f2-00a0c91efb8b}\properties

Opens key:

11e3-be65-806e6f6e6963}\

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

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

Queries value:

Queries value:

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

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

us[alternatecodepage]

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

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

Queries value:

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

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

Queries value: HKCU\software\microsoft\windows

nt\currentversion\appcompatflags[showdebuginfo]

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

options\dllnxoptions[usefilter]

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

options\dllnxoptions[2a3d6128a1b210860531603f74a24c7f.exe]
 Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]

Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[2a3d6128a1b210860531603f74a24c7f] Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\windows[loadappinit_dlls]

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

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

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

Queries value:

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

Queries value:

 $\label{thm:local_policies} \label{thm:local_policies} HKLM \label{thm:local_policies} In the constant of the$

Queries value:

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

Queries value:

 $\label{thm:local_explorer} \begin{tabular}{l} HKLM \begin{tabular}{l} HKLM \begin{tabular}{l} software \begin{tabular}{l} microsoft \begin{tabular}{l} windows \begin{tabular}{l} current version \begin{tabular}{l} policies \begin{tabular}{l} explorer \begin{tabular}{l} no set folders \begin{tabular}{l} policies \begin{tabular}{l} explorer \begin{tabular}{l} explo$

Queries value:

Queries value: HKLM\system\currentcontrol\set\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]

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

08002b30309d}\shellfolder[attributes]

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

 $08002b30309d \} \verb|\shellfolder[callforattributes]|$

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

08002b30309d}\shellfolder[restrictedattributes]

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

08002b30309d}\shellfolder[foldervalueflags]

Queries value:

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

08002b30309d}]

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

08002b30309d}\inprocserver32[]

Queries value:

 $\label{lem:hkcu} HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ \{d5291c64-7c88-11e3-be65-806e6f6e6963\} \ [data]$

Oueries value:

 $\label{lem:hkcu} \begin{tabular}{ll} \textbf{HKCU} software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\mountpoints2| cpc \verb|\currentversion| explorer expl$

11e3-be65-806e6f6e6963}[generation]

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

409d6c4515e9}[drivemask]

Queries value:

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

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

Queries 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]

Oueries value

 $\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} are \end{tabular} $$ is a parate process $$ is a$

Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling] HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden] Queries value: Queries value: Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons] 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: Oueries 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[nonetcrawling] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect] HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay] Queries value: $\label{thm:local_hammon} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced| [shows tatus bar] \end{tabular}$ HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-Oueries value: 97a27216f98a}\inprocserver32[] HKCR\directory[docobject] Oueries value: Oueries value: HKCR\folder[docobject] Queries value: HKCR\allfilesystemobjects[docobject] Queries value: HKCR\directory[browseinplace] HKCR\folder[browseinplace] Queries value: Oueries value: HKCR\allfilesystemobjects[browseinplace] Queries value: HKCR\directory[isshortcut] Queries value: HKCR\folder[isshortcut] HKCR\allfilesystemobjects[isshortcut] Queries value: HKCR\directory[alwaysshowext] Oueries value: Oueries value: HKCR\directory[nevershowext] Queries value: HKCR\folder[nevershowext] Queries value: HKCR\allfilesystemobjects[nevershowext] Queries value: HKCR\wow6432node\clsid\{75847177-f077-4171-bd2ca6bb2164fbd0}\inprocserver32[] HKLM\software\microsoft\com3[com+enabled] Oueries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[] Queries value: Oueries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\inprocserver32[inprocserver32] HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Queries value: b8dc300d9f9d}\inprocserver32[] Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\inprocserver32[threadingmodel] HKLM\software\microsoft\ole[maxsxshashcount] Queries value: Oueries value: db2c-424c-b029-7fe99a87c641}[category] Oueries value: db2c-424c-b029-7fe99a87c641}[name] Queries value: db2c-424c-b029-7fe99a87c641}[parentfolder] db2c-424c-b029-7fe99a87c641}[description] Oueries value: db2c-424c-b029-7fe99a87c641}[relativepath] Oueries value: db2c-424c-b029-7fe99a87c641}[parsingname]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-

Oueries value:

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

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

Oueries value:

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

Queries value:

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value

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

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]

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-continuous} HKLM \software \wow 6432 node \mbox{$1b$3ea5dc-b587-4786-b4ef-bd1dc332aeae} [description]$

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value

 $\label{thm:local-continuous} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f(1b3ea5dc-b587-4786-b4ef-bd1dc332eaea)\cite{localizedname}\cite{localizedname}$

Queries value:

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

Queries value:

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

Queries value:

Queries value:

 $HKLM\software\wow6432$ 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:

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

Queries value:

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

Oueries value:

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

Oueries value

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

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}]

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

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

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value

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

Queries value:

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

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}[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:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder 65f9-4cf6-a03a-e3ef65729f3d \cite{lem:hklmsoftware} [init folder handler]$

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

Queries value:

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

Oueries value:

Oueries value:

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

Oueries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1}{2} each \footnote{2}{2} - 4760 - 9 af \end{tikzpicture} e-a \footnote{2}{3} \footnote{2}{2} - 4760 - 9 af \end{tikzpicture} e-a \footnote{2}{3} \footnote{2}{2} - 4760 - 9 af \end{tikzpicture} e-a \footnote{2}{3} \footnote{2}{2} - 4760 - 9 \footnote{2} - 4760 - 9 \footnote{2}{2} - 4760 - 9 \footnote{2}{2} - 4760 - 9$

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:

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

Oueries value

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value

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

Queries value:

Queries value:

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

Queries value:

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

Oueries value

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

Queries value:

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

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]

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

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

Oueries value

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

Queries value:

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

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