# Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3311, Task ID: 751

Task ID: 751 Risk Level: 10

Date Processed: 2016-05-18 10:33:56 (UTC)

Processing Time: 62.2 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\2a29e3a5d469fbc803a504464393f98e.exe"

Sample ID: 3311
Type: basic
Owner: admin

Label: 2a29e3a5d469fbc803a504464393f98e

Date Added: 2016-05-18 10:30:49 (UTC)

File Type: PE32:win32:gui File Size: 1127085 bytes

MD5: 2a29e3a5d469fbc803a504464393f98e

SHA256: c16b99b6dd2073d18c21dc2a0a24ba4b99355ab89405e9abf1d902d7f841f5cd

Description: None

## Pattern Matching Results

10 Creates malicious mutex: DarkComet [APT, RAT]

Writes to memory of system processes

7 YARA score 7

5 Possible injector

4 Connects to local IP

7 Injects thread into Windows process

### Static Events

YARA rule hit: KeyLoggerStrings

Anomaly: PE: Contains a virtual section

### **Process/Thread Events**

Creates process: C:\windows\temp\2a29e3a5d469fbc803a504464393f98e.exe

 $["C:\windows\temp\2a29e3a5d469fbc803a504464393f98e.exe"\ ]$ 

Creates process: C:\Windows\SysWOW64\notepad.exe [notepad] Writes to process: PID:2912 C:\Windows\SysWOW64\notepad.exe

Creates remote thread: C:\Windows\SysWOW64\notepad.exe

## Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex: \Sessions\1\BaseNamedObjects\DC\_MUTEX-F5BOMXB
Creates mutex: \Sessions\1\BaseNamedObjects\DCPERSFWBP

## File System Events

Creates: C:\Users\Admin\AppData\Roaming\dclogs

Creates: C:\Users\Admin\AppData\Roaming\dclogs\2016-05-18-4.dc

Opens: C:\Windows\Prefetch\2A29E3A5D469FBC803A504464393F-7BFA99C0.pf

Opens: C:\Windows

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

Opens: C:\Windows\SysWOW64

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

Opens: C:\Windows\Temp\2a29e3a5d469fbc803a504464393f98e.exe

Opens: C:\Windows\WinSxS\x86\_microsoft.windows.common-

controls\_6595b64144ccf1df\_5.82.9200.16384\_none\_bf100cd445f4d954

 $Opens: C: \windows\winSxS\x86\_microsoft.windows.common-controls\_6595b64144ccf1df\_5.82.9200.16384\_none\_bf100cd445f4d954\comctl32.dl1$ 

Opens: C:\Windows\SysWOW64\winmm.dll
Opens: C:\Windows\SysWOW64\netapi32.dll

Opens:

 $C: \verb|Windows| winSxS| x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.9200.16384\_none\_ba245425e0986353$ 

Opens:

 Opens:
 C:\Windows\SysWOW64\msacm32.dll

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

 Opens:
 C:\Windows\SysWOW64\avicap32.dll

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

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

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

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

C:\Windows\SysWOW64\wkscli.dll Opens: Opens: C:\Windows\SysWOW64\msvfw32.dll C:\Windows\SysWOW64\msvcrt.dll Opens:

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\combase.dll C:\Windows\SysWOW64\oleaut32.dll Opens: Opens: C:\Windows\SysWOW64\advapi32.dll Opens: C:\Windows\SysWOW64\gdi32.dll C:\Windows\SysWOW64\user32.dll Opens: Opens: C:\Windows\SysWOW64\nsi.dll C:\Windows\SysWOW64\ws2\_32.dll Opens: C:\Windows\SysWOW64\ole32.dll Opens:

C:\Windows\SysWOW64\shlwapi.dll Opens: Opens: C:\Windows\SysWOW64\shell32.dll Opens: C:\Windows\SysWOW64\iertutil.dll Opens: C:\Windows\SysWOW64\wininet.dll C:\Windows\SysWOW64\urlmon.dll Opens: Opens: C:\Windows\SysWOW64\imm32.dll C:\Windows\SysWOW64\msctf.dll Opens:

Opens: C:\Windows\SysWOW64\en-US\msvfw32.dll.mui Opens: C:\Windows\SysWOW64\en-US\avicap32.dll.mui

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

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

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

Opens: C:\Windows\SysWOW64\en-US\user32.dll.mui

Opens: C:\

Opens: C:\Windows\SysWOW64\SHCore.dll Opens: C:\Windows\SysWOW64\notepad.exe

C:\Windows\Prefetch\NOTEPAD.EXE-1605FA5B.pf Opens:

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

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

4C77-AF34-C647E37CA0D9}.1.ver0x000000000000000e.db Opens: C:\Users\desktop.ini

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

Opens: C:\Windows\SysWOW64\en-US\setupapi.dll.mui

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

Opens: C:\Users\Admin\Desktop\desktop.ini Opens: C:\Windows\SysWOW64\winspool.drv

C:\Windows\WinSxS\x86\_microsoft.windows.common-Opens:

controls\_6595b64144ccf1df\_6.0.9200.16384\_none\_893961408605e985

C:\Windows\WinSxS\x86\_microsoft.windows.common-Opens:

controls\_6595b64144ccf1df\_6.0.9200.16384\_none\_893961408605e985\comctl32.dll

C:\Windows\SysWOW64\comdlg32.dll Opens:

Opens: C:\Windows\SysWOW64\en-US\notepad.exe.mui

C:\Windows\SysWOW64\mswsock.dll Opens: Opens: C:\Windows\WindowsShell.Manifest Opens: C:\Windows\Fonts\StaticCache.dat C:\Windows\SysWOW64\uxtheme.dll.Config Opens:

Opens: C:\Windows\Fonts\consola.ttf

Writes to: C:\Users\Admin\AppData\Roaming\dclogs\2016-05-18-4.dc

Reads from: C:\Windows\SysWOW64\notepad.exe

Reads from: C:\Users\desktop.ini

Reads from: C:\Users\Admin\Desktop\desktop.ini C:\Windows\Fonts\StaticCache.dat Reads from:

### Network Events

192.168.0.149:100

# Windows Registry Events

Creates key: Creates key: HKCU\software\dc3\_fexec Opens key: HKLM\software\microsoft\wow64

HKLM\system\currentcontrolset\control\terminal server Opens key: Opens key: HKLM\system\currentcontrolset\control\safeboot\option Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll

Opens kev:

HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers

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

Opens key: HKLM\system\currentcontrolset\control\nls\customlocale Opens key: HKLM\system\currentcontrolset\control\nls\language HKLM\system\currentcontrolset\control\mui\uilanguages Opens key: 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 kev:
                                    HKCU\
                                    HKCU\control panel\desktop\muicached\machinelanguageconfiguration
  Opens key:
  Opens key:
                                    HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
  Opens key:
                                    HKCU\software\policies\microsoft\control panel\desktop
                                    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:
  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
                                    HKLM\system\currentcontrolset\control\session manager
  Opens key:
  Opens kev:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  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 kev:
                                    HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
  Opens key:
                                    HKLM\system\currentcontrolset\control\lsa
  Opens key:
\label{thm:local_control} \begin{tabular}{ll} HKLM \end{tabular} which is the configuration of the configuration
  Opens key:
                                    HKLM\
  Opens key:
                                    HKLM\software\wow6432node\microsoft\ole
                                   HKLM\software\wow6432node\microsoft\ole\tracing
  Opens key:
  Opens key:
                                    HKLM\software\microsoft\ole\tracing
  Opens key:
                                    HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
                                    HKLM\software\wow6432node\microsoft\windows
  Opens key:
nt\currentversion\compatibility32
                                   HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
  Opens key:
compatibility
  Opens key:
                                    HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
                                   HKLM\software\wow6432node\microsoft\oleaut
  Opens key:
  Opens key:
                                    HKLM\system\currentcontrolset\services\lanmanworkstation\parameters
  Opens key:
                                    HKLM\system\currentcontrolset\control\cmf\config
  Opens key:
                                   HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
  Opens key:
                                    HKLM\software\wow6432node\microsoft\windows nt\currentversion\vfw
  Opens key:
                                    HKCU\software\borland\locales
                                   HKLM\software\wow6432node\borland\locales
  Opens key:
  Opens key:
                                    HKCU\software\borland\delphi\locales
  Opens key:
                                    HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:
                                   HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:
                                    HKLM\software\microsoft\sqmclient\windows
                                   HKLM\software\wow6432node\microsoft\windows
  Opens kev:
nt\currentversion\fontsubstitutes
                                   \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ fontsubstitutes
  Opens kev:
                                    HKLM\system\currentcontrolset\control\nls\sorting\ids
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\windows\currentversion\directmanipulation
  Opens key:
                                    HKLM\hardware\devicemap\video
  Opens key:
                                    f2223c917d28}\0000
  Opens key:
HKLM \ system \ current control set \ enum \ pci \ ven\_80ee \ dev\_beef \ subsys\_00000000 \ rev\_00 \ 3\&267a616a\&1\&10
  Opens key:
                                    HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:
                                    HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\086496d7
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
  Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
  Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
```

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000006

Opens kev:

Opens key:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
   Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ (catalog\_entries \ 0000000000101) \ (catalog\_entries \ (catalog \ (catalog\_entries \ (catalog \ (cata
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000
   Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
   Opens key:
                                             HKLM\software\wow6432node\microsoft\rpc
                                             HKLM\system\currentcontrolset\control\computername\activecomputername
   Opens key:
                                             HKLM\system\setup
   Opens key:
   Opens key:
                                             HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
   Opens key:
                                             HKLM\software\policies\microsoft\windows nt\rpc
                                             HKLM\system\currentcontrolset\control\idconfigdb
   Opens key:
   Opens key:
                                             HKLM \ system \ current control \ id configdb \ hardware \ profiles \ \ 0001
   Opens key:
                                             HKLM\system\currentcontrolset\control\idconfigdb\currentdockinfo
   Opens key:
Opens key:
c1bf-494e-b29c-65b732d3d21a}
   Opens kev:
c1bf-494e-b29c-65b732d3d21a}\propertybag
                                             HKLM\software\wow6432node\microsoft\windows\currentversion
   Opens key:
   Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{7c5a40ef-microsoft \ windows \ explorer \ \ \}
a0fb-4bfc-874a-c0f2e0b9fa8e}
   Opens key:
a0fb-4bfc-874a-c0f2e0b9fa8e}\propertybag
   Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ \ known foldersettings
   Opens kev:
                                             HKCU\software\dc3 fexec
   Opens key:
                                             HKCU\software\dc2 users
   Opens key:
                                             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\notepad.exe
   Opens key:
                                             HKLM\system\currentcontrolset\control\session manager\appcertdlls
   Opens key:
                                             HKLM\system\currentcontrolset\control\session manager\appcompatibility
                                             HKLM\software\wow6432node\policies\microsoft\windows\appcompat
   Opens key:
   Opens key:
                                             HKLM\software\policies\microsoft\windows\appcompat
                                             HKCU\software\microsoft\windows nt\currentversion
   Opens key:
                                             HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
   Opens key:
                                             HKLM\software\wow6432node\microsoft\windows
   Opens key:
nt\currentversion\appcompatflags
   Opens key:
                                             HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags\custom\notepad.exe
                                             HKCU\software\microsoft\windows\currentversion\explorer\shell folders
   Opens key:
                                             HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
   Opens kev:
   Opens key:
                                             HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\notepad.exe
   Opens key:
HKLM \label{lem:hklm} White the latest and the la
65f9-4cf6-a03a-e3ef65729f3d}
   Opens kev:
65f9-4cf6-a03a-e3ef65729f3d}\propertybag
                                             HKCU\software\microsoft\windows\currentversion\explorer
   Opens kev:
   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 kev:
```

HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer Opens key:  $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer$ 

Opens kev: HKCU\software\microsoft\windows\currentversion\policies\explorer

Opens key:

HKCU\software\classes\ Opens kev:

HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Opens key:

08002b30309d}\shellfolder

Opens kev:

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

08002b30309d}\shellfolder

Opens key:  $HKCU \ software \ microsoft \ windows \ current version \ explorer \ clsid \ \{20d04fe0-delta \ explorer \ ex$ 

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

Opens key:

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

a2d8-08002b30309d}\shellfolder

Opens key:  $\label{lem:hkcu} \verb+KKCU\+software\+microsoft\+windows\+currentversion\+policies\+nonenum$ 

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:

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

Opens key:

11e3-be65-806e6f6e6963}\

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

Opens key: HKCR\drive\shellex\folderextensions

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

4442-804e-409d6c4515e9}

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

409d6c4515e9}

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

Opens key: HKLM\software\policies\microsoft\windows\explorer Opens key: HKCU\software\policies\microsoft\windows\explorer HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-Opens key:

a6bb2164fbd0}\inprocserver32

Opens key: HKLM\software\microsoft\com3

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

Opens key: 

b8dc300d9f9d}

Opens key: HKCR\activatableclasses\clsid

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

b8dc300d9f9d}

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

b8dc300d9f9d}\treatas

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler32

Opens key:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{1f486a52 - 3cb1 - 48fd - 8f50 - 48fd - 8f50$ 

b8dc300d9f9d}\inprochandler

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

b8dc300d9f9d}\inprochandler

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

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

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}

HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-Opens key: 94f2-00a0c91efb8b}\properties

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

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

97a27216f98a}\inprocserver32

HKCU\software\classes\directory Opens key:

Opens key: HKCR\directory

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

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

Opens key: HKCR\folder

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

Opens key: HKCR\folder\shellex\iconhandler

HKCU\software\classes\allfilesystemobjects Opens kev:

Opens key: HKCR\allfilesystemobjects

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

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

Opens key: HKCR\directory\docobject

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

Opens key: HKCR\folder\docobject

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

 ${\tt HKCR\ left} lesystem objects \ \ \ docobject$ Opens key:

Opens kev:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mountpoints \\ 2 \setminus cpc \setminus volume \setminus \{d5291c63-7c88-1c40\} \\ 1 \setminus cpc \setminus volume \setminus \{d5291c63-7c88-1c40\} \\ 2 \setminus cpc \setminus volume \setminus \{d5291c63-7c88-1c40\} \\ 3 \setminus cpc \setminus volume \setminus \{d5291c63-7c88-1c40\} \\ 4 \setminus cpc \setminus volume \setminus \{d5291c63-1c40\} \\ 4 \setminus cpc \setminus volume \setminus \{d5291c63-1c40\} \\ 4 \setminus cpc \setminus \{$ 

11e3-be65-806e6f6e6963}\

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

HKCR\directory\browseinplace Opens key:

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

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

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

Opens key: HKCR\folder\clsid

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

HKCR\allfilesystemobjects\clsid Opens kev:

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{b4bfcc3a-bc1, b4bfcc3a-bc2, b4$ db2c-424c-b029-7fe99a87c641}

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

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

Opens key:

b587-4786-b4ef-bd1dc332aeae}\propertybag

HKLM\software\wow6432node\microsoft\rpc\extensions

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

HKLM\system\currentcontrolset\services\winsock\parameters Opens key: Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock

Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers

Opens kev: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip

Opens key: HKCU\software\microsoft\notepad

HKLM\software\wow6432node\microsoft\notepad\defaultfonts Opens key:

Opens key: HKLM\software\microsoft\notepad\defaultfonts Opens key: HKLM\system\currentcontrolset\control\nls\locale

Opens key: 

Opens key: HKLM\system\currentcontrolset\control\nls\language groups

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

Opens key: HKLM\software\microsoft\windows

nt\currentversion\languagepack\datastore\_v1.0

HKLM\software\microsoft\windows Opens key:  $\verb|nt\current| version \verb|\language| pack \verb|\surrogatefall| back |$ 

HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\segoe ui

Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat] HKLM\system\currentcontrolset\control\terminal server[tsuserenabled] Oueries value:

Oueries value:

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

Oueries value:

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

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] Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side \ [prefer external manifest]$ HKLM\system\currentcontrolset\control\nls\sorting\versions[] Oueries value:

HKCU\software\microsoft\windows Oueries value:

nt\currentversion\appcompatflags[showdebuginfo]

Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Oueries value:  $\label{lem:hklm} \verb+Kklm \+ software + microsoft + windows nt + current version + image file execution$ options\dllnxoptions[usefilter]

HKLM\software\microsoft\windows nt\currentversion\image file execution Oueries value: options\dllnxoptions[2a29e3a5d469fbc803a504464393f98e.exe]

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

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

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

Queries value: HKLM\software\microsoft\windows nt\currentversion\gre\_initialize[disablemetafiles]

HKLM\software\wow6432node\microsoft\windows Oueries value: nt\currentversion\compatibility32[2a29e3a5d469fbc803a504464393f98e] Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\windows[loadappinit\_dlls]

Queries value:

```
HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]
                      HKLM\system\currentcontrolset\control\cmf\config[system]
 Oueries value:
 Oueries value:
                      HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
 Oueries value:
                      HKLM\svstem\currentcontrolset\control\nls\customlocale[en-us]
 Queries value:
                      HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
 Queries value:
                      HKLM\software\microsoft\sqmclient\windows[ceipenable]
 Oueries value:
                      HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
shell dlg 2]
 Queries value:
                      HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
                      HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
 Oueries value:
 Queries value:
                      HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
 Queries value:
                      HKLM\hardware\devicemap\video[maxobjectnumber]
 Oueries value:
                      HKLM\hardware\devicemap\video[\device\video0]
 Queries value:
                      HKLM\system\currentcontrolset\control\class\{4d36e968-e325-11ce-bfc1-
08002be10318}\0000[pruningmode]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
 Oueries value:
Oueries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ catalog\_entries \ 00000000000008 \ [packed catalog item]
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000001[displaystring])
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000001[supported name space]]
 Queries value:
Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ (catalog\_entries \ 0000000000001 \ [version]
 Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ set \ name space\_catalog\_entries \ 000000000001[storesservice class in fo]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000002[librarypath]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
```

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[providerid]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[enabled]

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ name space\_catalog \ nam$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[addressfamily]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000002[supportednamespace]

Oueries value:

Queries value:

Queries value:

Oueries value:

Queries value:

Queries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[storesserviceclassinfo]

  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[librarypath]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[displaystring]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[providerid]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[addressfamily]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[supportednamespace]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[version]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[storesserviceclassinfo]
   Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ catalog\_entries \ 0000000000003 \ [provider info] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[librarypath] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[displaystring]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000004[providerid]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[addressfamily]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000004[supportednamespace]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[enabled]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[version] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[storesserviceclassinfo]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[librarypath]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[displaystring]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[providerid]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[addressfamily]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[supportednamespace]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[enabled]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[providerinfo]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[librarypath]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[providerid]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[addressfamily]
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ catalog\_entries \ 0000000000006 [supported namespace] \\ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[enabled]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[providerinfo]
  Oueries value:

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

Queries value:

HKLM\system\currentcontrolset\control\computername\activecomputername[computername]

Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup[systemsetupinprogress]
Queries value: HKLM\software\microsoft\rpc[idletimerwindow]

Queries value: HKLM\system\currentcontrolset\control\idconfigdb[currentconfig]

Queries value:

HKLM\system\currentcontrolset\control\idconfigdb\currentdockinfo[dockingstate]

Queries value: HKLM\system\currentcontrolset\control\idconfigdb\hardware

profiles\0001[hwprofileguid]

Queries value: HKLM\system\currentcontrolset\control\idconfigdb\hardware

profiles\0001[friendlyname]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} \ [category]$ 

Oueries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} \ [parent folder]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot \{905e63b6-c1bf-494e-b29c-65b732d3d21a\}\[description]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} [relative path]$ 

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma(905e63b6-c1bf-494e-b29c-65b732d3d21a)\gamma(parsingname)$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} [infotip]$ 

Oueries value:

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} [icon]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} \ [security]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} \ [stream resource]$ 

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[streamresourcetype]

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma\gamm$ 

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdesc$ 

Queries value:

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

Queries value:

Queries value:

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[foldertypeid]

Queries value:

 $\label{thm:local-bound} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\folderhandler]$ 

Queries value:

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version [program files dir]$ 

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} [name]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} [parent folder]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f(7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e)\f(description)\f$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{7c5a40effolder \ and \ baselines \ and \ and \ baselines \ and \ and$ 

a0fb-4bfc-874a-c0f2e0b9fa8e}[relativepath]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} [parsing name]$ 

Queries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} [localized name]$ 

Oueries value:

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

Oueries value:

 $\label{local-HKLM} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} [stream resource]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} [stream resource type]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} \ [local redirectonly]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} \ [roamable]$ 

Oueries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdesc$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} \ [stream]$ 

Queries value:

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

Queries value:

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\soft\windows\currentversion\explorer\folderdescriptions\folderdes$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdesc$ 

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]

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

folders[cache]

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[name]}$ 

Queries value:

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions \cite{lem:hklmsoftware} and \cite{lem:hklmso$ 

Queries value:

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

Queries value

 $\label{lem:hklmsoftwarewow6432node} HKLM \software \wow6432 node \mbox{$3eb685db-65f9-4cf6-a03a-e3ef65729f3d} \cite{Abcompart} \cite{Abcompart} \end{area} The label{lem:hklmsoftware} \end{area} The label{lem:hklmsoftware} \cite{Abcompart} \end{area} The label{lem:hklmsoftware} The label{lem:hklmsoftware} \end{area} The label{lem:hklmsoftware} \cite{Abcompart} \end{area} The label{lem:hklmsoftware} The label{lem:hklmsoftware} \end{area} The label{lem:hklmsoftware} The labe$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[infotip]} \\$ 

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\calebox{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[icon]$ 

Queries value:

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

Queries value:

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

Oueries value: 65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype] 65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly] Oueries value: 65f9-4cf6-a03a-e3ef65729f3d}[roamable] Oueries value: 65f9-4cf6-a03a-e3ef65729f3d}[precreate] Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[stream] Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath] Oueries value: 65f9-4cf6-a03a-e3ef65729f3d}[attributes] Queries value: 65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid] Queries value:  $HKLM \label{lem:hklm} Which is a constant with the statement of the stat$ 65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler] HKCU\software\microsoft\windows\currentversion\explorer\user shell Queries value: folders[appdata] Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer] Queries value:  $HKLM \ software \ microsoft \ windows \ current version \ policies \ \ explorer \ [no properties recyclebin]$ Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel] HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders] Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon] Queries value:  $HKLM \verb|\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]|$ Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[attributes] Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[callforattributes] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Queries value: 08002b30309d}\shellfolder[restrictedattributes] Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[foldervalueflags] Queries value: HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-08002b30309d}1 Queries value: HKCU\software\dc3\_fexec[{97e1de52-d6fa-11e1-be62-806e6f6e6963-1783083262}1 HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\inprocserver32[] Oueries value:  $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c64-7c88-4c144, d5291c64-7c88-4c144, d5291c64-$ 11e3-be65-806e6f6e6963}[data] HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-11e3-be65-806e6f6e6963}[generation] Queries value: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}[drivemask] HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-Queries value: a6bb2164fbd0}\inprocserver32[] HKLM\software\microsoft\com3[com+enabled] Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[] Queries value: Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\inprocserver32[inprocserver32] Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\inprocserver32[] HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Oueries value: b8dc300d9f9d}\inprocserver32[threadingmodel] Queries value: HKLM\software\microsoft\ole[maxsxshashcount] Oueries value:  $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [dontshow superhidden]$ 

HKCU\software\microsoft\windows\currentversion\explorer[shellstate]

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

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

Oueries value:

Oueries value:

Queries value:

Queries value:

HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess] HKLM\software\microsoft\windows\currentversion\setup[sourcepath] Oueries value: Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath] Queries value: 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] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext] Oueries value: Oueries value: 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:  $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ advanced\+ [webview]$ HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden] HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess] Queries value: Queries 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: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showstatusbar] HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-

97a27216f98a}\inprocserver32[]

Queries value: HKCR\directory[docobject]
Queries value: HKCR\folder[docobject]

Queries value: HKCR\allfilesystemobjects[docobject]

Queries value:

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

Queries value: HKCR\directory[browseinplace]
Queries value: HKCR\folder[browseinplace]

Queries value: HKCR\allfilesystemobjects[browseinplace]

Queries value:

11e3-be65-806e6f6e6963}[generation]

 Queries value:
 HKCR\directory[isshortcut]

 Queries value:
 HKCR\folder[isshortcut]

Queries value: HKCR\allfilesystemobjects[isshortcut]

Queries value: HKCR\directory[alwaysshowext]
Queries value: HKCR\directory[nevershowext]
Oueries value: HKCR\folder[nevershowext]

Queries value: HKCR\allfilesystemobjects[nevershowext]

Queries value:

 $\label{local-software-wow6432} HKLM\software\wow6432\\ node\windows\currentversion\explorer\folderdescriptions\begin{tabular}{l} b4bfcc3a-db2c-424c-b029-7fe99a87c641\\ \end{tabular} [category]$ 

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{localized} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\begin{tabular}{l} \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}[localized name] \end{tabular}$ 

Queries value:

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma\gamm$ 

Oueries value:

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

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

Oueries value:

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

Oueries value:

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

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3adb2c-424c-b029-7fe99a87c641}[roamable]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3adb2c-424c-b029-7fe99a87c641}[precreate]

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

folders[desktop]

Queries value:

b587-4786-b4ef-bd1dc332aeae}[category]

b587-4786-b4ef-bd1dc332aeae}[name]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dcb587-4786-b4ef-bd1dc332aeae}[parentfolder]

b587-4786-b4ef-bd1dc332aeae}[description]

b587-4786-b4ef-bd1dc332aeae}[relativepath]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dcb587-4786-b4ef-bd1dc332aeae}[parsingname]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dcb587-4786-b4ef-bd1dc332aeae}[infotip]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[localizedname]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dcb587-4786-b4ef-bd1dc332aeae}[icon]

Queries value:

b587-4786-b4ef-bd1dc332aeae}[security]

b587-4786-b4ef-bd1dc332aeae}[streamresource]

Queries value:

b587-4786-b4ef-bd1dc332aeae}[streamresourcetype]

b587-4786-b4ef-bd1dc332aeae}[localredirectonly]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1b3ea5dc-16b4e$ b587-4786-b4ef-bd1dc332aeae}[roamable]

b587-4786-b4ef-bd1dc332aeae}[precreate]

Queries value:

b587-4786-b4ef-bd1dc332aeae}[stream]

Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dcb587-4786-b4ef-bd1dc332aeae}[publishexpandedpath] b587-4786-b4ef-bd1dc332aeae}[attributes] Oueries value: b587-4786-b4ef-bd1dc332aeae}[foldertypeid] b587-4786-b4ef-bd1dc332aeae}[initfolderhandler] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}] Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll] Oueries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibilitv32[notepad] Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping] HKLM\system\currentcontrolset\services\winsock\setup Queries value: migration\providers\tcpip[winsock 2.0 provider id] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance] HKCU\software\microsoft\notepad[lfescapement] Queries value: HKCU\software\microsoft\notepad[lforientation] Oueries value: Queries value: HKCU\software\microsoft\notepad[lfweight] Queries value: HKCU\software\microsoft\notepad[lfitalic] Queries value: HKCU\software\microsoft\notepad[lfunderline] HKCU\software\microsoft\notepad[lfstrikeout] Queries value: Queries value: HKCU\software\microsoft\notepad[lfcharset] Oueries value: HKCU\software\microsoft\notepad[lfoutprecision] Queries value: HKCU\software\microsoft\notepad[lfclipprecision] Queries value: HKCU\software\microsoft\notepad[lfquality] Oueries value: HKCU\software\microsoft\notepad[lfpitchandfamily] HKLM\software\microsoft\notepad\defaultfonts[lffacename] Queries value: Queries value: HKLM\software\microsoft\notepad\defaultfonts[ipointsize] Oueries value: HKCU\software\microsoft\notepad[lffacename] HKCU\software\microsoft\notepad[ipointsize] Queries value: Oueries value: HKCU\software\microsoft\notepad[fwrap] Oueries value: HKCU\software\microsoft\notepad[statusbar] HKCU\software\microsoft\notepad[fsavewindowpositions] Oueries value: HKCU\software\microsoft\notepad[szheader] Queries value: Oueries value: HKCU\software\microsoft\notepad[sztrailer] Queries value: HKCU\software\microsoft\notepad[imargintop] Oueries value: HKCU\software\microsoft\notepad[imarginbottom] Oueries value: HKCU\software\microsoft\notepad[imarginleft] HKCU\software\microsoft\notepad[imarginright] Oueries value: Oueries value: HKCU\software\microsoft\notepad[iwindowposvl Oueries value: HKCU\software\microsoft\notepad[iwindowposx] HKCU\software\microsoft\notepad[iwindowposdx] Queries value: Oueries value: HKCU\software\microsoft\notepad[iwindowposdv] Queries value: HKCU\software\microsoft\notepad[fmle\_is\_broken]  $HKLM \verb|\system| current controlset| control \verb|\nls|| locale [00000409]$ Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\language groups[1] Oueries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\datastore\_v1.0[disable] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\datastore\_v1.0[datafilepath] HKLM\software\microsoft\windows Queries value: nt\currentversion\languagepack\surrogatefallback[plane1] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane2] HKLM\software\microsoft\windows Queries value: nt\currentversion\languagepack\surrogatefallback[plane3] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane4] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane5] HKLM\software\microsoft\windows Oueries value: nt\currentversion\languagepack\surrogatefallback[plane6] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane7] Queries value: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback[plane8]

nt\currentversion\languagepack\surrogatefallback[plane9]

nt\currentversion\languagepack\surrogatefallback[plane10]

Oueries value:

Queries value:

Queries value:

HKLM\software\microsoft\windows

HKLM\software\microsoft\windows

HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback[plane11] HKLM\software\microsoft\windows Queries value: nt\currentversion\languagepack\surrogatefallback[plane12] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane13] Queries value:  ${\it HKLM} \verb|\software\microsoft\windows|$ nt\currentversion\languagepack\surrogatefallback[plane14] HKLM\software\microsoft\windows Queries value: nt\currentversion\languagepack\surrogatefallback[plane15] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane16] Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]|$