Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3311, Task ID: 754

Task ID: 754 Risk Level: 10

Date Processed: 2016-05-18 10:34:11 (UTC)

Processing Time: 67.98 seconds IntelliVM Virtual Environment:

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

Sample ID: Type: admin Owner:

2a29e3a5d469fbc803a504464393f98e Label:

Date Added: 2016-05-18 10:30:49 (UTC) File Type: PE32:win32:gui

File Size: 1127085 bytes

2a29e3a5d469fbc803a504464393f98e MD5:

c16b99b6dd2073d18c21dc2a0a24ba4b99355ab89405e9abf1d902d7f841f5cd SHA256:

Description: None

Pattern Matching Results

Writes to memory of system processes

10 Creates malicious mutex: DarkComet [APT, RAT]

7 YARA score 7

Injects thread into Windows process

4 Connects to local IP

5 Possible injector

Static Events

YARA rule hit: KeyLoggerStrings

PE: Contains a virtual section Anomaly:

Process/Thread Events

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

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

Creates process: C:\Windows\SysWOW64\notepad.exe [notepad] PID:2272 C:\Windows\SysWOW64\notepad.exe Writes to process:

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

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex \Sessions\1\BaseNamedObjects\DC_MUTEX-F5B0MXB Creates mutex: \Sessions\1\BaseNamedObjects\DCPERSFWBP Creates mutex: Creates event: \KernelObjects\MaximumCommitCondition

File System Events

Opens:

Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches

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

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

Opens: C:\Windows

Opens: C:\Windows\System32\wow64.dll Opens: C:\Windows\System32\wow64win.dll Opens: C:\Windows\System32\wow64cpu.dll C:\Windows\system32\wow64log.dll Opens: Opens: C:\Windows\SysWOW64

Opens: C:\Windows\SysWOW64\sechost.dll Opens: C:\windows\temp\version.dll Opens: C:\Windows\SysWOW64\version.dll Opens: C:\windows\temp\wsock32.dll C:\Windows\SysWOW64\wsock32.dll Opens:

Opens: C:\windows\temp\2a29e3a5d469fbc803a504464393f98e.exe.Local\

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

controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af

C:\Windows\winsxs\x86_microsoft.windows.commoncontrols_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll

C:\Windows\SysWOW64\wkscli.dll

Opens: C:\windows\temp\winmm.dll Opens: C:\Windows\SysWOW64\winmm.dll C:\windows\temp\netapi32.dll Opens: C:\Windows\SysWOW64\netapi32.dll Opens: C:\windows\temp\netutils.dll Opens: C:\Windows\SysWOW64\netutils.dll Opens: Opens: C:\windows\temp\srvcli.dll C:\Windows\SysWOW64\srvcli.dll Opens: Opens: C:\windows\temp\wkscli.dll

```
Opens:
```

C:\windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80

Opens:

Opens:

C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll

Opens: C:\windows\temp\msacm32.dll C:\Windows\SysWOW64\msacm32.dll Opens: Opens: C:\windows\temp\SHFolder.dll Opens: C:\Windows\SysWOW64\shfolder.dll C:\windows\temp\AVICAP32.DLL Opens: Opens: C:\Windows\SysWOW64\avicap32.dll Opens: C:\windows\temp\MSVFW32.dll Opens: C:\Windows\SysWOW64\msvfw32.dll

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

 Opens:
 C:\windows\temp\2a29e3a5d469fbc803a504464393f98e.ENU

 Opens:
 C:\windows\temp\2a29e3a5d469fbc803a504464393f98e.ENU.DLL

 Opens:
 C:\windows\temp\2a29e3a5d469fbc803a504464393f98e.EN

 Opens:
 C:\windows\temp\2a29e3a5d469fbc803a504464393f98e.EN.DLL

C:\Windows\SysWOW64\imm32.dll

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

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

Opens: C:\Windows\SysWOW64\rpcss.dll
Opens: C:\windows\temp\PSymSE8rHgHi.dcp

Opens: C:\

Opens: C:\Windows\SysWOW64\PSymSE8rHgHi\

Opens: C:\Program Files (x86)
Opens: C:\Windows\SysWOW64\notepad

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

C:\Windows\System32\DriverStore\FileRepository\tkbtnpn.inf_061cd165\lencins.dll

Opens: C:\Program Files (x86)\Common Files\Microsoft Shared\Ink\mshwusa.dll

controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2

Opens: C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll

Opens: C:\Windows\SysWOW64\winspool.drv
Opens: C:\Users\Admin\AppData\Roaming

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

Opens: C:\Windows\SysWOW64\shell32.dll
Opens: C:\Windows\WindowsShell.Manifest

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

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

Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db

Opens: C:\windows\temp\ntmarta.dll
Opens: C:\Windows\SysWOW64\ntmarta.dll

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

4C77-AF34-C647E37CA0D9}.1.ver0x000000000000001.db
Opens: C:\Users\desktop.ini
Opens: C:\Users

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

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

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

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

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

 Opens:
 C:\Windows\SysWOW64\WSHTCPIP.DLL

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

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

Reads from: C:\Windows\Fonts\StaticCache.dat
Reads from: C:\Windows\SysWOW64\notepad.exe
Reads from: C:\Users\desktop.ini

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

Network Events

Connects to: 192.168.0.149:100

Windows Registry Events

Creates key: HKCU\software
Creates key: HKCU\software\dc3_fexec

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

options

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

Opens key: HKLM\software\microsoft\wow64

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

execution options

Opens key: HKLM\system\currentcontrolset\control\terminal server
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

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

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

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

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

Opens key: HKCU\

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

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

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

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

Opens key:

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

Opens key: HKLM\system\currentcontrol\set\control\nls\sorting\versions

Opens key: HKLM\

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

nt\currentversion\diagnostics

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

nt\currentversion\gre_initialize

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

nt\currentversion\compatibility32

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

compatibility

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

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\wow6432node\microsoft\oleaut
Opens key: HKLM\system\currentcontrolset\services\crypt32

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

settings Opens kev:

HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings

 $Opens\ key: \\ HKLM\software\policies\microsoft\windows\currentversion\internet$

settings

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

Opens key: HKLM\software\wow6432node\borland\locales
Opens key: HKCU\software\borland\delphi\locales

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

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

nt\currentversion\fontsubstitutes

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

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

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

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

Opens key: HKLM\software\microsoft\windows

nt\currentversion\languagepack\datastore_v1.0

Opens key: HKLM\software\microsoft\windows

 $\verb|nt\currentversion\languagepack\surrogatefall back|$

Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\segoe ui Opens key: HKLM\hardware\devicemap\video

Opens key: HKLM\system\currentcontrol\video\{43056cc8-3bf6-4ce7-bd67-

1e1a187c13e9}\0000

Opens key:

 $HKLM \ system \ current control set \ enum \ pci \ ven_80ee \ dev_beef \ subsys_00000000 \ rev_00 \ \ 3\&267a616a\&0\&10$

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

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

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
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000003
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
 Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
 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\00000000010
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
 Opens key:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000003
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
 Opens key:
Opens key:
                 HKLM\software\wow6432node\microsoft\rpc
 Opens key:
                 Opens key:
                 HKLM\system\setup
                 HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
 Opens key:
 Opens key:
                 HKLM\software\policies\microsoft\windows nt\rpc
                  HKLM\system\currentcontrolset\control\idconfigdb
 Opens key:
 Opens key:
                 HKLM\system\currentcontrolset\control\idconfigdb\hardware profiles\0001
 Opens key:
                 HKLM\system\currentcontrolset\control\idconfigdb\currentdockinfo
 Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ \ folder descriptions
 Opens key:
c1bf-494e-b29c-65b732d3d21a}
 Opens kev:
c1bf-494e-b29c-65b732d3d21a}\propertybag
 Opens key:
                 HKLM\software\wow6432node\microsoft\windows\currentversion
 Opens key:
a0fb-4bfc-874a-c0f2e0b9fa8e}
a0fb-4bfc-874a-c0f2e0b9fa8e}\propertybag
 Opens key:
HKLM \setminus software \setminus wow6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus known folders \\ ettings
 Opens key:
                 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 kev:
                  HKLM\system\currentcontrolset\control\session manager\appcompatibility
 Opens key:
                  HKLM\software\wow6432node\policies\microsoft\windows\appcompat
```

HKLM\software\policies\microsoft\windows\appcompat

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

HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers

 $\label{local-operator} \mbox{HKCU\software\mbox{\sc microsoft\windows} nt\current\version\app\compatflags\layers} \\$

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\notepad.exe

Opens key:

Opens key:

Opens key:

Opens key:

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ between the constant \ folder \ between the constant \ folder \ fold$

65f9-4cf6-a03a-e3ef65729f3d}

65f9-4cf6-a03a-e3ef65729f3d}\propertybag

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

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

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ 2a29e3a5d469fbc803a504464393f98e. exemple \ applications \$

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: $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus (20d04fe0-derivative for the context of the context of$

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

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ clsid \ \{20d04fe0-3aea-1069-4044fe0-3aea-1060-4044fe0-3aea-1060-4044fe0-3aea-1060-4044fe0-3aea-1060-4044f$

a2d8-08002b30309d}\shellfolder

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \policies \nonenum \policies \nonenum \policies \polici$ Opens kev:

Opens key:

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

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

Opens key:

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

Opens kev:

11e3-a68e-806e6f6e6963}\

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

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}

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

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

Opens key: HKLM\software\microsoft\com3

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

b8dc300d9f9d}

HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\treatas

 $\label{local-back} $HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treat as $$ \end{array} $$ $HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treat as $$ \end{array} $$ $$ $HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treat as $$ \end{array} $$ $$ $$ $HKCR\wow6432node\clsid\$ Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{1f486a52 - 3cb1 - 48fd - 8f50 - 48fd - 8f50$ Opens key:

b8dc300d9f9d}\progid

 $HKCR \setminus box{432} node \\ clsid \\ \{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\} \\ \setminus progid$ Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\}$

Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} Opens key:

b8dc300d9f9d}\progid

Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid

Opens key: $HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{1f486a52 - 3cb1 - 48fd - 8f50 - 48fd - 8f50$

b8dc300d9f9d}\inprocserv er32

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprochandler32 Opens key:

HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler

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

b8dc300d9f9d}\inprochandler

Opens key:

Opens key: HKLM\software\microsoft\windows\currentversion\setup Opens key: HKLM\svstem\currentcontrolset\control\lsa\accessproviders

Opens key: HKLM\system\currentcontrolset\services\ldap

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

Opens key: HKCU\software\microsoft\notepad

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

Opens key: $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| notepad\\| default fonts$

Opens kev:

 $HKLM \label{lem:hklm} Which is the large state of the large state of$

Opens key:

11e3-a68e-806e6f6e6963}\

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

Opens kev:

 $\label{thm:local_hammon_hammon} \begin{tabular}{l} HKCU \software \microsoft \windows \shell \associations \urlassociations \directory \end{tabular}$

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

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

Opens key: HKCR\directory\curver
Opens key: HKCR\directory\

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

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

Opens key: HKCR\folder

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

Opens key: HKCR\folder\shellex\iconhandler

Opens key: HKCU\software\classes\allfilesystemobjects

Opens key: HKCR\allfilesystemobjects

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

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

Opens key: HKCR\directory\docobject

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

Opens key: HKCR\folder\docobject

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

Opens key: HKCR\allfilesystemobjects\docobject

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

Opens key: HKCR\directory\browseinplace

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

Opens key: HKCR\folder\browseinplace

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

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

Opens key: HKCR\directory\clsid

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

Opens key: HKCR\folder\clsid

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

Opens key: HKCR\allfilesystemobjects\clsid

Opens key:

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

Opens kev:

Opens key:

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

Opens key:

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

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

Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock

 $Opens\ key: \\ HKLM \ system \ current controls et \ services \ winsock \ setup\ migration \ providers$

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

migration\providers\tcpip

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

options[disableusermodecallbackfilter]

Queries value: HKLM\system\currentcontrolset\control\session

manager[cwdillegalindllsearch]

Queries value: HKLM\system\currentcontrol\set\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrol\set\control\terminal server[tsuserenabled]

Queries value:

 $\label{lem:hklm} HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled] \\ Queries\ value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]$

Queries value:

 $HKLM \verb|\system| current controlset \verb|\control| nls \verb|\language[install]| anguage fallback]$

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

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:

 $HKLM \label{lem:hklm} Which is the like the li$

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

Queries value: HKLM\system\currentcontrol\session manager[safedllsearchmode]

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

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

```
HKLM\software\wow6432node\microsoft\windows
 Oueries value:
nt\currentversion\windows[loadappinit_dlls]
 Oueries value:
                      HKLM\software\microsoft\ole[pageallocatorusesystemheap]
 Queries value:
                      HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
                      HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
 Oueries value:
 Queries value:
                      settings[disableimprovedzonecheck]
                      HKLM\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[security_hklm_only]
 Queries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]
 Queries value:
                      HKLM\system\currentcontrolset\control\cmf\config[system]
 Oueries value:
                      HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
 Queries value:
                      HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
 Queries value:
                      HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
 Oueries value:
                      HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
shell dlg 2]
 Queries value:
                      HKLM\system\currentcontrolset\control\nls\locale[00000409]
                      HKLM\system\currentcontrolset\control\nls\language groups[1]
 Oueries value:
                      HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\datastore_v1.0[disable]
                      HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
                      HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane1]
                      HKLM\software\microsoft\windows
 Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane2]|
                      HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane3]
                      HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane4]
                      HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane5]
 Oueries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
 Oueries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
                      HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane8]
 Oueries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
                      HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane10]
                      HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane11]
 Queries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
 Oueries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
 Oueries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
 Queries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
                      HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane16]
 Queries value:
                      HKLM\hardware\devicemap\video[maxobjectnumber]
 Oueries value:
                      HKLM\hardware\devicemap\video[\device\video3]
                      Oueries value:
1e1a187c13e9}\0000[pruningmode]
                      HKLM\software\microsoft\sqmclient\windows[ceipenable]
 Queries value:
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
 Oueries value:
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\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
 Oueries 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\000000000001[librarypath] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\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\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Oueries value:
- 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:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
- 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\00000000003[displaystring] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerid]
 Queries 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:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 0000000000003 \ [enabled] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
 Oueries value:
- $HKLM \system \current control set \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \$
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 0000000000003 \ [provider info] \ Oueries \ value:$
- 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] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[providerid]
 Queries value:
- $HKLM \system \current control set \services \winsock 2 \parameters \names pace_catalog 5 \catalog_entries \names family] \\ Queries value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[enabled]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[version]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries \ 000000000004 \ [storesserviceclassinfo] \ Queries \ value:$

```
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap services \setminus mame space\_catalog \\ \setminus catalog\_entries \setminus 00000000000004[provider info]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[librarypath]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000005 \ [displaystring]
   Queries 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\00000000005[addressfamily]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000005[supported name space]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[version]
   Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[displaystring]
Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ (catalog\_entries \ 000000000006 \ [address family]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ set alog\_entries \ (00000000000006 \ [version]) \ and \ (version) \ and \ (ve
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
                                            HKLM\software\microsoft\rpc[maxrpcsize]
   Queries value:
   Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
                                            HKLM\svstem\setup[oobeinprogress]
   Oueries value:
   Queries value:
                                            HKLM\system\setup[systemsetupinprogress]
                                            \label{lem:hklm} \verb+kklm \+ system \+ control \+ idconfigdb \+ [current config]
   Oueries value:
   Queries value:
HKLM \setminus system \setminus current control \setminus idconfigdb \setminus current dockinfo[docking state]
   Queries value:
                                            HKLM \setminus system \setminus current control \setminus idconfigdb \setminus hardware
profiles\0001[hwprofileguid]
  Queries value:
                                            HKLM\system\currentcontrolset\control\idconfigdb\hardware
profiles\0001[friendlyname]
  Oueries value:
c1bf-494e-b29c-65b732d3d21a}[category]
  Oueries value:
c1bf-494e-b29c-65b732d3d21a}[name]
   Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ (905e63b6-1000) \ descriptions \ (905e63b6-10000) \ descriptions \ (905e63b6-10000) \ descriptions \ (905e63b6-10000) \ de
c1bf-494e-b29c-65b732d3d21a}[parentfolder]
  Queries value:
c1bf-494e-b29c-65b732d3d21a}[description]
   Oueries value:
c1bf-494e-b29c-65b732d3d21a}[relativepath]
  Queries value:
```

c1bf-494e-b29c-65b732d3d21a}[parsingname]

c1bf-494e-b29c-65b732d3d21a}[infotip]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-

Oueries value:

c1bf-494e-b29c-65b732d3d21a}[localizedname]

Oueries value:

c1bf-494e-b29c-65b732d3d21a}[icon]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-

c1bf-494e-b29c-65b732d3d21a}[security]

Oueries value:

c1bf-494e-b29c-65b732d3d21a}[streamresource]

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

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:

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

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\soft\windows\currentversion\explorer\folderdescriptions\footnote{1.5} Accorded to the soft of t$

Queries value:

Oueries value:

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

Queries value:

Queries value:

 $HKLM\software\slashed wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdesc$

Queries value:

Oueries value:

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

Queries value:

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

Queries value:

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

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

Oueries value:

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

Queries value:

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

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[cache]

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

options[disablelocaloverride]

Queries value: HKCU\software\dc3_fexec[{846ee340-7039-11de-9d20-806e6f6e6963-

216485478}]

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

Queries value:

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

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

nt\currentversion\compatibility32[notepad]

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

folders[appdata]
Queries value:

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

Queries value:

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

```
Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
    Oueries value:
                                                       HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
                                                       HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Oueries value:
08002b30309d}\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[wantsfordisplay]
                                                       HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
08002b30309d}\shellfolder[hidefolderverbs]
   Queries value:
                                                       HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[usedrophandler]
                                                       HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
08002b30309d}\shellfolder[wantsforparsing]
                                                       HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
                                                       HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[queryforoverlay]
                                                       HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
08002b30309d}\shellfolder[mapnetdriveverbs]
                                                       HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Oueries value:
08002b30309d}\shellfolder[queryforinfotip]
                                                       HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[hideinwebview]
                                                       HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
08002b30309d}\shellfolder[hideondesktopperuser]
                                                       HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Oueries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
                                                       HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[wantsuniversaldelegate]
                                                       HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[nofilefolderjunction]
    Oueries value:
                                                       08002b30309d}\shellfolder[pintonamespacetree]
                                                       HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[hasnavigationenum]
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{20d04fe0-3aea-1069-a2d8-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{20d04fe0-3aea-1069-a2d8-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{20d04fe0-3aea-1069-a2d8-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{20d04fe0-3aea-1069-a2d8-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{20d04fe0-3aea-1069-a2d8-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{20d04fe0-3aea-1069-a2d8-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{20d04fe0-3aea-1069-a2d8-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{20d04fe0-3aea-1069-a2d8-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{20d04fe0-3aea-1069-a2d8-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{20d04fe0-3aea-1069-a2d8-microsoft \setminus windows \setminus current version \setminus policies \setminus pol
08002b30309d}]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d4-8213-
11e3-a68e-806e6f6e6963}[data]
    Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ (8063a3d4-8213-100) \ mountpoints \ 2 \ cpc \ volume \ (8063a3d4-8213-100) \ mountpoints \ 2 \ cpc \ volume \ (8063a3d4-8213-100) \ mountpoints \ 2 \ cpc \ volume \ (8063a3d4-8213-100) \ mountpoints \ 2 \ cpc \ volume \ (8063a3d4-8213-100) \ mountpoints \ 2 \ cpc \ volume \ (8063a3d4-8213-100) \ mountpoints \ 2 \ cpc \ volume \ (8063a3d4-8213-100) \ mountpoints \ 2 \ cpc \ volume \ (8063a3d4-8213-100) \ mountpoints \ 2 \ cpc \ volume \ (8063a3d4-8213-100) \ mountpoints \ 2 \ cpc \ volume \ (8063a3d4-8213-100) \ mountpoints \ 2 \ cpc \ volume \ (8063a3d4-8213-100) \ mountpoints \ 2 \ cpc \ volume \ (8063a3d4-8213-100) \ mountpoints \ 2 \ cpc \ volume \ (8063a3d4-8213-100) \ mountpoints \ 2 \ cpc \ volume \ (8063a3d4-8213-100) \ mountpoints \ 2 \ cpc \ volume \ (8063a3d4-8213-100) \ mountpoints \ 2 \ cpc \ 2 \ cp
11e3-a68e-806e6f6e6963}[generation]
                                                       HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
    Queries value:
409d6c4515e9}[drivemask]
    Queries value:
                                                       HKLM\software\microsoft\com3[com+enabled]
                                                       HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
    Queries value:
    Oueries value:
                                                       HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[inprocserver32]
                                                       HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
    Queries value:
b8dc300d9f9d}\inprocserver32[]
    Oueries value:
                                                       HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[threadingmodel]
                                                       HKLM\software\microsoft\ole[maxsxshashcount]
    Oueries value:
                                                       HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
    Queries value:
                                                       HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
    Oueries value:
    Queries value:
HKLM \setminus system \setminus current control \\ \setminus lsa \setminus access providers [martaextension]
    Queries value:
                                                       HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
                                                       HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
    Oueries value:
    Queries value:
                                                       HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
    Queries value:
                                                       HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
    Queries value:
                                                       HKCU\software\microsoft\notepad[lfescapement]
```

Oueries value: HKCU\software\microsoft\notepad[lforientation] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu] Queries value: Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

HKCU\software\microsoft\notepad[lfweight] Queries value: Oueries value: HKCU\software\microsoft\notepad[lfitalic] Oueries value: HKCU\software\microsoft\notepad[lfunderline] Queries value: HKCU\software\microsoft\notepad[lfstrikeout] Queries value: HKCU\software\microsoft\notepad[lfcharset] HKCU\software\microsoft\notepad[lfoutprecision] Oueries value: Queries value: HKCU\software\microsoft\notepad[lfclipprecision] Queries value: HKCU\software\microsoft\notepad[lfquality] HKCU\software\microsoft\notepad[lfpitchandfamily] Oueries value:

Queries value:

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

Queries value:

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

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

Oueries value:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced [show superhidden]$

Oueries value:

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

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

Oueries value:

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

Oueries value:

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

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

Oueries value:

11e3-a68e-806e6f6e6963}[data]

Queries value:

11e3-a68e-806e6f6e6963}[generation]

Oueries value: Queries value: HKLM\software\microsoft\notepad\defaultfonts[ipointsize]

Oueries value: HKCU\software\microsoft\notepad[lffacename] Queries value: HKCU\software\microsoft\notepad[ipointsize] HKCU\software\microsoft\notepad[fwrap] Oueries value: Oueries value: HKCU\software\microsoft\notepad[statusbar]

Oueries value: HKCU\software\microsoft\notepad[fsavewindowpositions] Queries value: HKCU\software\microsoft\notepad[szheader]

Oueries value: HKCU\software\microsoft\notepad[sztrailer] Queries value: HKCU\software\microsoft\notepad[imargintop] HKCU\software\microsoft\notepad[imarginbottom] Oueries value: Oueries value: HKCU\software\microsoft\notepad[imarginleft] Oueries value: HKCU\software\microsoft\notepad[imarginright] HKCU\software\microsoft\notepad[iwindowposy] Queries value: Queries value: HKCU\software\microsoft\notepad[iwindowposx] Oueries value: HKCU\software\microsoft\notepad[iwindowposdx] HKCU\software\microsoft\notepad[iwindowposdy] Queries value: Queries value: HKCU\software\microsoft\notepad[fmle_is_broken]

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

Queries value: HKCR\allfilesystemobjects[docobject] Oueries value: HKCR\directory[browseinplace] Queries value: HKCR\folder[browseinplace]

HKCR\allfilesystemobjects[browseinplace] Oueries value:

Queries value: HKCR\directory[isshortcut] Oueries value: HKCR\folder[isshortcut]

Oueries value: HKCR\allfilesystemobjects[isshortcut] Oueries value: HKCR\directory[alwaysshowext]

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

Queries value: HKCR\allfilesystemobjects[nevershowext]

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma_{bbfcc3a-db2c-424c-b029-7fe99a87c641}[streamresourcetype]$

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

Queries value:

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

folders[desktop]

Queries value:

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

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:

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[relativepath]}$

Queries value

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[infotip]}$

Queries value

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

Queries value:

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

Oueries value:

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

Oueries value

Oueries value:

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

 $\label{thm:local-basis} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1} b3ea5dc-b587-4786-b4ef-bd1dc332 aeae \footnote{1} [stream]$

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

 $\label{thm:local-basis} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1} b587-4786-b4ef-bd1dc332 aeae \cite{1} [initfolder \cite{1} handler]$

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

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

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

Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]

Queries value:

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

Queries value: HKLM\system\currentcontrolset\services\winsock\setup

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:

Queries value:

 $HKLM \verb|\system| current controlset \verb|\services| tcpip \verb|\parameters| winsock[helperdllname]$