Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 9, Task ID: 33

Task ID: 33 Risk Level: 5

Date Processed: 2016-04-28 12:46:48 (UTC)

Processing Time: 62.58 seconds
Virtual Environment: IntelliVM

 $\label{lem:c:windows} \textbf{Execution Arguments:} \qquad \textbf{"c:windows} \textbf{temp} \textbf{83323edb74ebd75cdc7ef98e3daddd07.exe} \textbf{and the control of the cont$

Sample ID: 9
Type: basic
Owner: admin

Label: 83323edb74ebd75cdc7ef98e3daddd07

Date Added: 2016-04-28 12:44:50 (UTC)
File Type: PE32:win32:gui

File Type: PE32:win32:gui File Size: 368272 bytes

MD5: 83323edb74ebd75cdc7ef98e3daddd07

SHA256: c56d96269d96d7a66021934c404ec40b89008c51c80760a96c6b25ce307b3183

Description: None

Pattern Matching Results

2 PE: Nonstandard section

5 Packer: UPX

5 PE: Contains compressed section

Static Events

Anomaly: PE: Contains a virtual section

Anomaly: PE: Contains one or more non-standard sections

Packer: UPX

Process/Thread Events

Creates process: C:\windows\temp\83323edb74ebd75cdc7ef98e3daddd07.exe

["C:\windows\temp\83323edb74ebd75cdc7ef98e3daddd07.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex:

 $\verb|\Sessions|1| BaseNamedObjects| 83323edb74ebd75cdc7ef98e3daddd07.exej97KThLU| and the session of the context of the context$

Creates semaphore: \Sessions\1\BaseNamedObjects\INI-83323edb74ebd75cdc7ef98e3daddd07.data

Creates semaphore: \Sessions\1\BaseNamedObjects\GR_FileChecker

Creates semaphore: \Sessions\1\BaseNamedObjects\GRO

Creates semaphore: \Sessions\1\BaseNamedObjects\GR_FlushingList \Creates semaphore: \Sessions\1\BaseNamedObjects\GR_Write

Creates semaphore: \Sessions\1\BaseNamedObjects\GR_GErrMsg
Creates semaphore: \Sessions\1\BaseNamedObjects\GR1

\Sessions\1\BaseNamedObjects\GR2 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR3 Creates semaphore: \Sessions\1\BaseNamedObjects\GR4 \Sessions\1\BaseNamedObjects\GR5 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR6 Creates semaphore: \Sessions\1\BaseNamedObjects\GR7 \Sessions\1\BaseNamedObjects\GR8 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR9 Creates semaphore: \Sessions\1\BaseNamedObjects\GR10 \Sessions\1\BaseNamedObjects\GR11 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR12 Creates semaphore: \Sessions\1\BaseNamedObjects\GR13

Creates semaphore: \Sessions\1\BaseNamedObjects\GR14
Creates semaphore: \Sessions\1\BaseNamedObjects\GR15
Creates semaphore: \Sessions\1\BaseNamedObjects\GR16
Creates semaphore: \Sessions\1\BaseNamedObjects\GR17
Creates semaphore: \Sessions\1\BaseNamedObjects\GR18
Creates semaphore: \Sessions\1\BaseNamedObjects\GR19

Creates semaphore: \Sessions\1\BaseNamedObjects\GR20
Creates semaphore: \Sessions\1\BaseNamedObjects\GR21
Creates semaphore: \Sessions\1\BaseNamedObjects\GR22
Creates semaphore: \Sessions\1\BaseNamedObjects\GR23
Creates semaphore: \Sessions\1\BaseNamedObjects\GR23

Creates semaphore: \Sessions\1\BaseNamedObjects\GR25
Creates semaphore: \Sessions\1\BaseNamedObjects\GR26
Creates semaphore: \Sessions\1\BaseNamedObjects\GR27
Creates semaphore: \Sessions\1\BaseNamedObjects\GR28
Creates semaphore: \Sessions\1\BaseNamedObjects\GR29

Creates semaphore: \Sessions\1\BaseNamedObjects\GR30
Creates semaphore: \Sessions\1\BaseNamedObjects\GR31
Creates semaphore: \Sessions\1\BaseNamedObjects\GR32

Creates semaphore: \Sessions\1\BaseNamedObjects\GR32
Creates semaphore: \Sessions\1\BaseNamedObjects\GR33

\Sessions\1\BaseNamedObjects\GR34 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR35 $\verb|\Sessions|1\\BaseNamedObjects|GR36|$ Creates semaphore: \Sessions\1\BaseNamedObjects\GR37 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR38 Creates semaphore: $\Sessions\1\BaseNamedObjects\GR39$ \Sessions\1\BaseNamedObjects\GR40 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR41 \Sessions\1\BaseNamedObjects\GR42 Creates semaphore: \Sessions\1\BaseNamedObjects\GR43 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR44 \Sessions\1\BaseNamedObjects\GR45 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR46 \Sessions\1\BaseNamedObjects\GR47 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR48 \Sessions\1\BaseNamedObjects\GR49 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR50 Creates semaphore: \Sessions\1\BaseNamedObjects\GR51 Creates semaphore: \Sessions\1\BaseNamedObjects\GR52 Creates semaphore: \Sessions\1\BaseNamedObjects\GR53 Creates semaphore: \Sessions\1\BaseNamedObjects\GR54 \Sessions\1\BaseNamedObjects\GR55 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR56 Creates semaphore: \Sessions\1\BaseNamedObjects\GR57 Creates semaphore: \Sessions\1\BaseNamedObjects\GR58 \Sessions\1\BaseNamedObjects\GR59 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR60 Creates semaphore: \Sessions\1\BaseNamedObjects\GR61 Creates semaphore: \Sessions\1\BaseNamedObjects\GR62 Creates semaphore: \Sessions\1\BaseNamedObjects\GR63 Creates semaphore: \Sessions\1\BaseNamedObjects\GR64 \Sessions\1\BaseNamedObjects\GR65 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR66 Creates semaphore: \Sessions\1\BaseNamedObjects\GR67 Creates semaphore: \Sessions\1\BaseNamedObjects\GR68 Creates semaphore: \Sessions\1\BaseNamedObjects\GR69 Creates semaphore: \Sessions\1\BaseNamedObjects\GR70 \Sessions\1\BaseNamedObjects\GR71 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR72 Creates semaphore: \Sessions\1\BaseNamedObjects\GR73 \Sessions\1\BaseNamedObjects\GR74 Creates semaphore: Creates semaphore: $\Sessions\1\BaseNamedObjects\GR75$ Creates semaphore: \Sessions\1\BaseNamedObjects\GR76 \Sessions\1\BaseNamedObjects\GR77 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR78 Creates semaphore: \Sessions\1\BaseNamedObjects\GR79 \Sessions\1\BaseNamedObjects\GR80 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR81 \Sessions\1\BaseNamedObjects\GR82 Creates semaphore: \Sessions\1\BaseNamedObjects\GR83 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR84 Creates semaphore: \Sessions\1\BaseNamedObjects\GR85 Creates semaphore: \Sessions\1\BaseNamedObjects\GR86 Creates semaphore: \Sessions\1\BaseNamedObjects\GR87 Creates semaphore: \Sessions\1\BaseNamedObjects\GR88 $\verb|\Sessions|1\BaseNamedObjects|| GR89$ Creates semaphore: \Sessions\1\BaseNamedObjects\GR90 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR91 \Sessions\1\BaseNamedObjects\GR92 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR93 Creates semaphore: \Sessions\1\BaseNamedObjects\GR94 Creates semaphore: \Sessions\1\BaseNamedObjects\GR95 Creates semaphore: \Sessions\1\BaseNamedObjects\GR96 Creates semaphore: \Sessions\1\BaseNamedObjects\GR97 \Sessions\1\BaseNamedObjects\GR98 Creates semaphore: $\verb|\Sessions|1\\BaseNamedObjects|GR99|$ Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR100

Creates semaphore: \Sessions\1\BaseNamedObjects\INI-83323edb74ebd75cdc7ef98e3daddd07.data0

File System Events

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

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

Creates:

 $\verb| C:\Users\land Admin\land PpData\Roaming\land GetRightToGo\$3323edb74ebd75cdc7ef98e3daddd07.data Creates: \\$

Opens: C:\Windows

```
C:\Windows\System32\wow64.dll
  Opens:
                                       C:\Windows\SysWOW64
  Opens:
                                       C:\Windows\SysWOW64\apphelp.dll
  Opens:
                                       C:\Windows\Temp\83323edb74ebd75cdc7ef98e3daddd07.exe
  Opens:
  Opens:
                                       C:\Windows\SysWOW64\ntdll.dll
  Opens:
                                       C:\Windows\SysWOW64\kernel32.dll
                                       C:\Windows\SysWOW64\KernelBase.dll
  Opens:
  Opens:
                                       C:\Windows\apppatch\sysmain.sdb
                                       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
  Opens:
                                       C:\Windows\SysWOW64\oledlg.dll
  Opens:
                                       C:\Windows\SysWOW64\secur32.dll
  Opens:
                                       C:\Windows\SysWOW64\winspool.drv
                                       C:\Windows\SysWOW64\sechost.dll
  Opens:
  Opens:
                                       C:\Windows\SysWOW64\combase.dll
  Opens:
                                       C:\Windows\SysWOW64\SHCore.dll
  Opens:
                                       C:\Windows\SysWOW64\msvcrt.dll
                                       C:\Windows\SysWOW64\bcryptprimitives.dll
  Opens:
  Opens:
                                       C:\Windows\SysWOW64\cryptbase.dll
  Opens:
                                       C:\Windows\SysWOW64\sspicli.dll
  Opens:
                                       C:\Windows\SysWOW64\rpcrt4.dll
  Opens:
                                       C:\Windows\SysWOW64\advapi32.dll
  Opens:
                                       C:\Windows\SysWOW64\user32.dll
                                       C:\Windows\SysWOW64\gdi32.dll
  Opens:
  Opens:
                                       C:\Windows\SysWOW64\shlwapi.dll
  Opens:
                                       C:\Windows\SysWOW64\shell32.dll
                                       C:\Windows\SysWOW64\comdlg32.dll
  Opens:
  Opens:
                                       C:\Windows\SysWOW64\ole32.dll
  Opens:
                                       C:\Windows\SysWOW64\oleaut32.dll
  Opens:
                                       C:\Windows\SysWOW64\nsi.dll
  Opens:
                                       C:\Windows\SysWOW64\ws2_32.dll
  Opens:
                                       C:\Windows\SysWOW64\imm32.dll
  Opens:
                                       C:\Windows\SysWOW64\msctf.dll
  Opens:
                                       C:\Windows\WindowsShell.Manifest
  Opens:
                                       C:\Windows\SysWOW64\uxtheme.dll
  Opens:
                                       C:\windows\temp\83323edb74ebd75cdc7ef98e3daddd07.exe.2.Manifest
  Opens:
                                       C:\windows\temp\83323edb74ebd75cdc7ef98e3daddd07.exe.3.Manifest
  Opens:
                                       C:\windows\temp\83323edb74ebd75cdc7ef98e3daddd07.exe.Config
  Opens:
                                       \verb|C:\wedge windows \mid temp \ 83323edb74ebd75cdc7ef98e3daddd07.exe.1000. Manifest| \\
  Opens:
  Opens:
                                       C:\Users\Admin\AppData\Local
                                       C:\Windows\SysWOW64\tzres.dll
  Opens:
  Opens:
                                       C:\Windows\SysWOW64\en-US\tzres.dll.mui
  Opens:
                                       C:\Windows\Fonts\tahoma.ttf
                                       {\tt C:\Windows\Globalization\Sorting\SortDefault.nls}
  Opens:
  Opens:
                                       C:\Windows\Fonts\StaticCache.dat
                                       C:\Windows\SysWOW64\clbcatq.dll
  Opens:
  Opens:
                                       C:\Windows\SysWOW64\propsys.dll
                                       Opens:
4C77-AF34-C647E37CA0D9}.1.ver0x00000000000000e.db
  Opens:
                                      C:\Users\desktop.ini
  Opens:
                                       C:\Windows\SysWOW64\cfgmgr32.dll
  Opens:
                                       C:\Windows\SysWOW64\devobj.dll
  Opens:
                                       C:\Windows\SysWOW64\setupapi.dll
  Opens:
                                       C:\Users
  Opens:
                                       C:\Users\Admin
                                       C:\Users\Admin\Desktop\desktop.ini
  Opens:
  Opens:
                                       C:\Users\Admin\AppData
  Opens:
                                       C:\Users\Admin\AppData\Roaming\GetRightToGo
  Opens:
C:\Users\Admin\AppData\Roaming\GetRightToGo\83323edb74ebd75cdc7ef98e3daddd07.data
  Opens:
                                       C:\Windows\Temp
  Opens:
C: \verb|Vsers| Admin| AppData| Roaming | GetRightToGo| 83323edb74ebd75cdc7ef98e3daddd07.data0| GetRightToGo| GetRig
  Opens:
                                      C:\Windows\SysWOW64\ntmarta.dll
                                       C:\Users\Admin\Desktop
  Opens:
  Opens:
                                       C:\Users\Admin\Desktop\Downloads\
  Opens:
                                       C:\Windows\SysWOW64\dwmapi.dll
  Opens:
                                       C:\Users\Admin\Documents\desktop.ini
  Opens:
                                       C:\Users\Public\desktop.ini
  Opens:
                                       C:\Users\Public
  Opens:
                                       C:\Users\Public\Desktop\desktop.ini
  Opens:
                                       C:\Windows\Fonts\sserife.fon
  Writes to:
C:\Users\Admin\AppData\Roaming\GetRightToGo\83323edb74ebd75cdc7ef98e3daddd07.data0
  Reads from:
                                      C:\Windows\Fonts\StaticCache.dat
  Reads from:
                                       C:\Users\desktop.ini
  Reads from:
                                       C:\Users\Admin\Desktop\desktop.ini
  Reads from:
                                       C:\Windows\Temp\83323edb74ebd75cdc7ef98e3daddd07.exe
```

Reads from:

C:\Users\Admin\AppData\Roaming\GetRightToGo\83323edb74ebd75cdc7ef98e3daddd07.data

Reads from:

C:\Users\Admin\AppData\Roaming\GetRightToGo\83323edb74ebd75cdc7ef98e3daddd07.data0

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

Windows Registry Events

HKCU\software\headlight Creates key:

Creates key: HKCU\software\headlight\getrighttogo

HKCU\software\headlight\getrighttogo\sharedconfig Creates key: HKCU\software\headlight\getrighttogo\customizedapps Creates kev:

Opens key: HKLM\software\microsoft\wow64

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

Opens key:

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

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

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

HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete Opens key:

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

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

Opens key: HKCU\

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

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

HKCU\control panel\desktop Opens key:

HKCU\control panel\desktop\muicached Opens kev:

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog Opens kev:

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

nt\currentversion\appcompatflags\disable8and16bitmitigation

Opens key:

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

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

Opens key: $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \ nt \setminus current version \setminus image \ file$

execution options

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

Opens key:

HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions

Opens key:

HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy

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

Opens key:

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

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

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:

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

Opens key: HKLM\software\microsoft\ole

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

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

HKCU\software\classes\ Opens key:

Opens key: HKCU\software\classes\wow6432node\clsid

Opens key: HKCR\wow6432node\clsid

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

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

Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ policies\+ network$ Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\policies\comdlg32

Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr

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

Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername

Opens key: HKLM\system\setup

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

 $\label{locale} \verb|HKLM\| system \| current controls et \| control \| nls \| locale \| alternate sorts \| control \| sorts \| control \| contro$ Opens kev:

Opens key: HKLM\system\currentcontrolset\control\nls\language groups Opens key: HKCU\software\microsoft\windows\currentversion\directmanipulation Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids Opens key: Opens key: HKLM\software\wow6432node\microsoft\ctf\ Opens key: HKLM\software\wow6432node\microsoft\ctf\knownclasses HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\datastore_v1.0 HKLM\software\microsoft\windows Opens kev: nt\currentversion\languagepack\surrogatefallback Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\ms shell dlg 2 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\2cdb6258 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005 Opens kev: Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003 Opens kev: Opens key: Opens kev: Opens kev: Opens key: Opens key: Opens kev: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001 Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004 Opens key: Opens key: Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer Opens kev: Opens key: Opens kev:

db2c-424c-b029-7fe99a87c641}

Opens kev:

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

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

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

Opens kev:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in folders$

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

folders Opens kev:

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

08002b30309d}\shellfolder

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

08002b30309d}\shellfolder

Opens kev:

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

Opens kev:

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

a2d8-08002b30309d}\shellfolder

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

Opens kev:

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

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

08002b30309d}\inprocserver32

Opens key:

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

Opens key:

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

11e3-be65-806e6f6e6963}\

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

Opens key: HKCR\drive\shellex\folderextensions

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

4442-804e-409d6c4515e9}

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

409d6c4515e9}

Opens key: $HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| windows\\| explorer$

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

a6bb2164fbd0}\inprocserver32

HKLM\software\microsoft\com3 Opens key:

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

Opens key:

b8dc300d9f9d}

Opens key:

Opens key: HKCR\activatableclasses\clsid

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

Opens key:

 $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{1f486a52 - 3cb1 - 48fd - 8f50 - 48fd - 8f50$ b8dc300d9f9d}\treatas HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas Opens kev:

HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}

 $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{1f486a52 - 3cb1 - 48fd - 8f50 - 48fd - 8f50$ Opens key: b8dc300d9f9d}\inprocserv er32

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

b8dc300d9f9d}\inprocserver32

Opens key:

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler

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

b8dc300d9f9d}\inprochandler

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

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

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

97a27216f98a}\inprocserver32

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

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

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

HKCR\folder Opens key:

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

Opens key: HKCR\folder\shellex\iconhandler

Opens key: HKCU\software\classes\allfilesystemobjects

Opens key: HKCR\allfilesystemobjects

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

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 kev: 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

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

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\wow6432node\microsoft\windows\currentversion\setup

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

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

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

94f2-00a0c91efb8b}

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

94f2-00a0c91efb8b}\properties

Opens key: HKCU\software

Opens key:

11e3-be65-806e6f6e6963}\

Opens key

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-

65f9-4cf6-a03a-e3ef65729f3d}

Opens key

 $\label{thm:local-continuous} HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685db-1642\} \\ des$

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

Opens key

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-

b587-4786-b4ef-bd1dc332aeae}

Opens key:

 $HKL \dot{M} \setminus soft \dot{w} are \\ \ wow 6432 node \\ \ microsoft \\ \ windows \\ \ current version \\ \ explorer \\ \ folder descriptions \\ \ \{1b3ea5dc-164444, 164444, 16444, 16444, 16444, 16444, 16444, 16444, 16444, 16444, 16444$

 $b587-4786-b4ef-bd1dc332aeae \} \verb|\property| bag$

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

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

Opens key: HKLM\system\currentcontrol\sa\accessproviders

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{fdd39ad0-microsoft \ windows \ explorer \ folder \ descriptions \ explorer \ folder \ descriptions \ explorer \ folder \ folder \ folder \ fines \ folder \ folder$

238f-46af-adb4-6c85480369c7}

Opens key:

 $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f(fdd39ad0-fd039ad0-f$

238f-46af-adb4-6c85480369c7}\propertybag

Opens key: HKCU\software\classes\wow6432node\clsid\{59031a47-3f72-44a7-89c5-

5595fe6b30ee}\shellfolder

Opens key: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-

5595fe6b30ee}\shellfolder

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{59031a47-

3f72-44a7-89c5-5595fe6b30ee}\shellfolder

Opens key:

89c5-5595fe6b30ee}\shellfolder

Opens key: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-

5595fe6b30ee}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{4df0c730-df9d-4ae3-9153-

aa6b82e9795a}\inprocserver32

Opens key:

 $HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \cal{eq:c4aa340d-c4aaa340d-c4aaa340d-c4aaa340d-c4aaa340d-c4aaa340d-c4aaa340d-c4aaa340d-c4aaaaa40d-c4aaaaaaaaaaaaaaaaaaaaaaaaaaaa$

f20f-4863-afef-f87ef2e6ba25}

Opens key:

 $f20f-4863-afef-f87ef2e6ba25\} \setminus property bag$

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

shell folders

Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\ms sans serif

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

Oueries value:

Queries value:

 $HKLM \setminus system \setminus current control \\ language[installlanguagefallback]$

Queries value: HKLM\system\currentcontrol\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:

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

Queries value: HKCU\software\microsoft\windows

 $\verb|nt\currentversion\appcompatflags[showdebuginfo]|\\$

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

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[83323edb74ebd75cdc7ef98e3daddd07.exe]

```
Oueries value:
                         HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
                         HKLM \verb|\system| current controlset| control \verb|\lag| fips algorithm policy]
 Oueries value:
 Oueries value:
                         HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
                         HKLM\software\wow6432node\microsoft\windows
 Oueries value:
nt\currentversion\compatibility32[83323edb74ebd75cdc7ef98e3daddd07]
 Queries value:
                         HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit dlls]
 Queries value:
                         HKLM\software\microsoft\ole[pageallocatorusesystemheap]
 Oueries value:
                         HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
 Oueries value:
                         HKLM\software\microsoft\ole[aggressivemtatesting]
 Queries value:
                         HKLM\software\microsoft\sqmclient\windows[ceipenable]
 Oueries value:
                         HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
 Oueries value:
                         HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
 Queries value:
                         HKLM\system\currentcontrolset\control\nls\customlocale[en]
 Queries value:
                         HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
 Queries value:
                         HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
 Queries value:
HKLM\system\setup[oobeinprogress]
 Queries value:
 Queries value:
                         HKLM\system\setup[systemsetupinprogress]
                         HKLM\system\currentcontrolset\control\nls\locale[00000409]
 Queries value:
 Queries value:
                         HKLM\system\currentcontrolset\control\nls\language groups[1]
 Queries value:
                         HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
 Queries value:
                         HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
                         HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
 Queries value:
 Queries value:
                         HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
 Oueries value:
                         HKLM\software\microsoft\windows
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]
 Oueries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
 Oueries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
                         HKLM\software\microsoft\windows
 Queries value:
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]
 Oueries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
 Oueries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
 Oueries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
 Oueries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
 Oueries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
                         HKLM\software\microsoft\windows
 Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane15]|
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane16]
 Queries 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]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
 Oueries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 0000000000003 \ [packed catalog item]
 Queries value:
```

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ (0000000000004 [packed catalog item]) \ details \$

Queries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[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\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\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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace] Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \namespace_catal$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[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:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 00000000000002 [providerid] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
 Queries value:
- 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\0000000000002[storesserviceclassinfo]

 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath] Queries 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]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[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\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath] Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 0000000000004 \ [displaystring] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
 Oueries 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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
 Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog \ set alog_entries \ 000000000000004 \ [version]$

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[storesserviceclassinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[providerinfo] Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog \ (catalog_entries \ 00000000005[library path])$ Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000005 \ [displaystring]$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerid] Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000005 \ [address family]$ Oueries value:

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\000000000005[version] Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog \ set in \ services \ winsock 2 \ parameters \ names \ pace_catalog \ entries \ 00000000000005 \ [storesserviceclass \ info]$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[librarypath] Queries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 000000000006 \ [displaystring]$ Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap amespace_catalog \\ S \setminus catalog_entries \setminus 0000000000006[providerid]$ Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 000000000006 \ [address family]$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog \ set alog_entries \ (00000000000006 \ [enabled]) \ (enabled)$ Oueries value:

Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap services \setminus ser$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]

Oueries value:

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

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

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

Oueries value:

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

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

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

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

```
db2c-424c-b029-7fe99a87c641}[security]
    Oueries value:
db2c-424c-b029-7fe99a87c641}[streamresource]
    Oueries value:
db2c-424c-b029-7fe99a87c641}[streamresourcetype]
    Oueries value:
db2c-424c-b029-7fe99a87c641}[localredirectonly]
    Oueries value:
db2c-424c-b029-7fe99a87c641}[roamable]
    Oueries value:
db2c-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:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{b4bfcc3a-bc1, b4bfcc3a-bc1, b4
db2c-424c-b029-7fe99a87c641}[foldertypeid]
    Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b
db2c-424c-b029-7fe99a87c641}[initfolderhandler]
    Queries value:
                                                                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[desktop]
    Queries value:
                                                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
                                                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
08002b30309d}\shellfolder[callforattributes]
    Oueries value:
                                                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[restrictedattributes]
                                                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
08002b30309d}\shellfolder[foldervalueflags]
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}1
                                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Oueries value:
08002b30309d}\inprocserver32[]
    Queries value:
HKCU \ software \ icrosoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c64-7c88-4cq24, d5291c64-7c88-4cq24, d5291c64-7c86-7c88-4cq24, d5291c64-7c86-7c86-7c86-7c
11e3-be65-806e6f6e6963}[data]
    Queries value:
11e3-be65-806e6f6e6963}[generation]
    Queries value:
                                                                    HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
                                                                  HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-
    Oueries value:
a6bb2164fbd0}\inprocserver32[]
    Queries value:
                                                                  HKLM\software\microsoft\com3[com+enabled]
                                                                   HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
    Oueries value:
    Oueries value:
                                                                   HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[inprocserver32]
                                                                  HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
    Queries value:
b8dc300d9f9d}\inprocserver32[]
    Queries value:
                                                                  HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[threadingmodel]
    Queries value:
                                                                   HKLM\software\microsoft\ole[maxsxshashcount]
HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
    Queries value:
                                                                   HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [nowebview]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
    Queries value:
                                                                   HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
    Oueries value:
Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
    Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ advanced \ advanced \ advanced \ advanced \ adva
```

Oueries value:

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

Oueries value:

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

Queries value:

 $\label{thm:linear_had} \begin{tabular}{ll} HKCU \software \mbox{\mathbb{N} indows \current version} \end{tabular} advanced \mbox{\mathbb{M} indows} \end{tabular} \begin{tabular}{ll} HKCU \software \mbox{\mathbb{M} indows} \end{tabular}$

Oueries value:

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

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

Queries value:

Queries value:

 $\label{thm:linear} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{thm:linear} separate process \cite{thm:linear} advanced \cite{thm:linear} separate \$

Oueries value:

 $\label{lem:hccu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced[nonetcrawling]| \\ \end{tabular}$

Oueries value:

 $\label{lem:hkcu} \begin{tabular}{ll} \textbf{HKCU} software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced[autocheckselect]| \end{tabular}$

Queries value:

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

Queries value:

 $\label{lem:hcu} \begin{tabular}{ll} HKCU software \verb|microsoft| windows \verb|currentversion| explorer \verb|advanced| [showtypeoverlay] \\ \end{tabular}$

Queries value:

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

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

Queries value: HKCR\allfilesystemobjects[browseinplace]

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

Queries value: HKCR\allfilesystemobjects[isshortcut]

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

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

Queries value: HKCR\allfilesystemobjects[nevershowext]

Queries value: HKCU\software\headlight\getrighttogo\sharedconfig[useloadimage]

Queries value:

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

Oueries value:

 $HKCU \setminus software \\ \mbox{\current version} \\ \mbox{\current version}$

11e3-be65-806e6f6e6963}[generation]

Queries value: HKCU\software\headlight\getrighttogo\sharedconfig[doxpthemes]

Queries value:

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

Queries value:

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

Queries value: KLM\software

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \mbox{$3eb685db-65f9-4cf6-a03a-e3ef65729f3d} [parent folder]$

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\flocalizednamel

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ before \ folder \ folde$

65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]

Oueries value:

65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]

Oueries value:

65f9-4cf6-a03a-e3ef65729f3d}[roamable]

Oueries value:

65f9-4cf6-a03a-e3ef65729f3d}[precreate]

Oueries value:

 $HKLM \label{lem:hklm} White the latest and the la$ 65f9-4cf6-a03a-e3ef65729f3d}[stream]

Oueries value:

65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]

Oueries value:

65f9-4cf6-a03a-e3ef65729f3d}[attributes]

Queries value:

65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]

Oueries value:

65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]

Queries value: folders[appdata]

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

Queries value:

b587-4786-b4ef-bd1dc332aeae}[category]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[name]

Queries value:

b587-4786-b4ef-bd1dc332aeae}[parentfolder]

Oueries value:

 $HKLM \label{lem:hklm} White the latest and the la$ b587-4786-b4ef-bd1dc332aeae}[description]

Queries value:

b587-4786-b4ef-bd1dc332aeae}[relativepath]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[parsingname]

Queries value:

b587-4786-b4ef-bd1dc332aeae}[infotip]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[localizedname]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[icon]

Oueries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1b3ea5dc-b2b4a2b4b2ab4b2a2$ b587-4786-b4ef-bd1dc332aeae}[streamresource]

Queries value:

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

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[localredirectonly]

Queries value:

 $HKLM \label{lem:hklm} White the latest and the la$ b587-4786-b4ef-bd1dc332aeae}[roamable]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[precreate]

Oueries value:

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

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[publishexpandedpath]

Oueries value:

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

Oueries value:

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

b587-4786-b4ef-bd1dc332aeae}[foldertypeid]

Oueries value:

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

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

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

Oueries value:

HKLM\software\policies\microsoft\windows\system[copyfilebufferedsynchronousio]

Queries value:

HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]

Queries value: HKCU\software\headlight\getrighttogo\sharedconfig[debug]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} \ [category]$

Queries value:

 $\label{lem:hklmsoftwarewow6432} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \fdd 39 ad 0-238 f-46 af-ad b4-6 c85480 369 c7 \[name \]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} [parent folder]$

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(fdd39ad0-238f-46af-adb4-6c85480369c7)\f(description)\f(desc$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} [relative path]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} [parsing name]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} \ [infotip]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} [localized name]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} \ [icon]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} \ [Folder description \ explorer \ folder descriptions] \ fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} \ [Folder description \ explorer \ folder descriptions] \ fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} \ [Folder description \ explorer \ folder descriptions] \ fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} \ [Folder description \ explorer \ folder descriptions] \ fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} \ [Folder description \ explorer \ folder descriptions] \ fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} \ [Folder description \ explorer \ folder descriptions] \ fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} \ [Folder description \ explorer \ folder descriptions] \ fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} \ [Folder description \ explorer \ folder descriptions] \ fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} \ [Folder description \ explorer \ folder descriptions] \ fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} \ [Folder description \ explorer \ folder descriptions] \ fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} \ [Folder description \ explorer \ folder descriptions] \ fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} \ [Folder description \ explorer \ folder description \ explorer \ folder description \ explorer \ folder \ folde$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} [stream resource]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(fdd39ad0-238f-46af-adb4-6c85480369c7)\f(streamresourcetype)\f(streamres$

Queries value:

 $\label{thm:localization} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fdd 39 ad 0-238f-46 af-ad b4-6c85480369 c7 \[local redirectionly]$

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fdd 39 ad 0-238f-46 af-ad b4-6c85480 369 c7 \[roamable]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{fdd39ad0-238f-46af-adb4-6c85480369c7\}[precreate]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \fdd 39 ad 0-238f-46af-ad b4-6c85480369 \color="list-ream" list-ream \folder descriptions \fdd 39 ad 0-238f-46af-ad b4-6c85480369 \color="list-ream" list-ream \folder descriptions \fdd 39 ad 0-238f-46af-ad b4-6c85480369 \color="list-ream" list-ream \folder descriptions \fdd 39 ad 0-238f-46af-ad b4-6c85480369 \color="list-ream" list-ream \folder descriptions \folds \fdd 39 ad 0-238f-46af-ad b4-6c85480369 \color="list-ream" list-ream \folds \fold$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(fdd39ad0-238f-46af-adb4-6c85480369c7)\f(publishexpandedpath)\f(publishexpandedp$

Queries value:

 $\label{local-prop} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7\}\ [attributes]}$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{fdd39ad0-238f-46af-adb4-6c85480369c7\} \ [folder typeid]$

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[initfolderhandler]

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

folders[personal]

Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-

5595fe6b30ee}\shellfolder[attributes]

Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-

5595fe6b30ee}\shellfolder[callforattributes]

Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-

5595fe6b30ee}\shellfolder[restrictedattributes]

Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-

5595fe6b30ee}\shellfolder[foldervalueflags]

Oueries value:

HKLM\software\microsoft\windows\currentversion\policies\nonenum[{59031a47-3f72-44a7-89c5-

5595fe6b30ee}1

Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-

5595fe6b30ee}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{4df0c730-df9d-4ae3-9153-

aa6b82e9795a}\inprocserver32[]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} \ [category]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} \ [name]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} \ [parent folder]$

Queries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} [relative path]$

Oueries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{c4aa340d-f20f-4863-afef-f87ef2e6ba25\}[infotip]$

Queries value:

Queries value:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \{c4aa340d-f20f-4863-afef-f87ef2e6ba25\}[icon]$

Queries value:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} [security]$

Queries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{c4aa340d-f20f-4863-afef-f87ef2e6ba25\}[stream resource type]$

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\\folderdescriptions\\\{c4aa340d-f20f-4863-afef-f87ef2e6ba25\}[precreate]$

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{c4aa340d-f20f-4863-afef-f87ef2e6ba25\}[publish expanded path]$

Queries value:

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

Queries value:

Queries value:

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

Queries value:

 $\label{thm:local_explorer} \begin{tabular}{ll} HKLM \label{thm:local_explorer} Iturn of fspian imations \end{tabular}$

Sets/Creates value

HKCU\software\headlight\getrighttogo\customizedapps[83323edb74ebd75cdc7ef98e3daddd07]
Sets/Creates value: HKCU\software\headlight\getrighttogo\sharedconfig[busypause]
Sets/Creates value: HKCU\software\headlight\getrighttogo\sharedconfig[filecache]
Sets/Creates value: HKCU\software\headlight\getrighttogo\sharedconfig[filecachekb]
Sets/Creates value: HKCU\software\headlight\getrighttogo\sharedconfig[rollback]
Sets/Creates value: HKCU\software\headlight\getrighttogo\sharedconfig[dotgetright]