Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 145, Task ID: 580

Task ID: 580 Risk Level:

Date Processed: 2016-04-28 13:03:06 (UTC)

Processing Time: 61.14 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\090ae821aa4e2bd4bddeb0cb6466b181.exe"

Sample ID: Type: basic Owner: admin

090ae821aa4e2bd4bddeb0cb6466b181 Label:

Date Added: 2016-04-28 12:45:05 (UTC)

PE32:win32:gui File Type: File Size: 368304 bytes

090ae821aa4e2bd4bddeb0cb6466b181 MD5:

f4579402cf6d8d5e7c6e8feaa08a34027c3336fc789d27b1392725806af19e21 SHA256:

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:

Process/Thread Events

Creates process: C:\windows\temp\090ae821aa4e2bd4bddeb0cb6466b181.exe

["C:\windows\temp\090ae821aa4e2bd4bddeb0cb6466b181.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex:

Creates semaphore:

Creates semaphore:

\Sessions\1\BaseNamedObjects\090ae821aa4e2bd4bddeb0cb6466b181.exermVZRFow

Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0

\Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1 Creates mutex: Creates event: \Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1

Creates event: \KernelObjects\MaximumCommitCondition

Creates semaphore: $\verb|\Sessions| 1 \\ BaseNamedObjects \\ INI-090ae 821aa 4e2bd4bddeb 0cb 6466b181.data \\ Abstraction of the context of the contex$

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

\Sessions\1\BaseNamedObjects\GR1 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR2 Creates semaphore: \Sessions\1\BaseNamedObjects\GR3 \Sessions\1\BaseNamedObjects\GR4 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR5 Creates semaphore: \Sessions\1\BaseNamedObjects\GR6 \Sessions\1\BaseNamedObjects\GR7 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR8 Creates semaphore: \Sessions\1\BaseNamedObjects\GR9 \Sessions\1\BaseNamedObjects\GR10 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR11 Creates semaphore: \Sessions\1\BaseNamedObjects\GR12 \Sessions\1\BaseNamedObjects\GR13 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR14 Creates semaphore: \Sessions\1\BaseNamedObjects\GR15 Creates semaphore: \Sessions\1\BaseNamedObjects\GR16 Creates semaphore: \Sessions\1\BaseNamedObjects\GR17 \Sessions\1\BaseNamedObjects\GR18 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR19 \Sessions\1\BaseNamedObjects\GR20 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR21 Creates semaphore: \Sessions\1\BaseNamedObjects\GR22 Creates semaphore: \Sessions\1\BaseNamedObjects\GR23 Creates semaphore: \Sessions\1\BaseNamedObjects\GR24 Creates semaphore: \Sessions\1\BaseNamedObjects\GR25 \Sessions\1\BaseNamedObjects\GR26 Creates semaphore: \Sessions\1\BaseNamedObjects\GR27 Creates semaphore:

\Sessions\1\BaseNamedObjects\GR28

\Sessions\1\BaseNamedObjects\GR29

\Sessions\1\BaseNamedObjects\GR30 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR31 \Sessions\1\BaseNamedObjects\GR32 Creates semaphore: \Sessions\1\BaseNamedObjects\GR33 Creates semaphore: \Sessions\1\BaseNamedObjects\GR34 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR36 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR37 Creates semaphore: \Sessions\1\BaseNamedObjects\GR38 Creates semaphore: \Sessions\1\BaseNamedObjects\GR39 \Sessions\1\BaseNamedObjects\GR40 Creates semaphore: Creates semaphore: $\Sessions\1\BaseNamedObjects\GR41$ Creates semaphore: \Sessions\1\BaseNamedObjects\GR42 \Sessions\1\BaseNamedObjects\GR43 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR44 Creates semaphore: \Sessions\1\BaseNamedObjects\GR45 \Sessions\1\BaseNamedObjects\GR46 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR47 Creates semaphore: \Sessions\1\BaseNamedObjects\GR48 Creates semaphore: \Sessions\1\BaseNamedObjects\GR49 Creates semaphore: \Sessions\1\BaseNamedObjects\GR50 Creates semaphore: \Sessions\1\BaseNamedObjects\GR51 \Sessions\1\BaseNamedObjects\GR52 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR53 Creates semaphore: \Sessions\1\BaseNamedObjects\GR54 Creates semaphore: \Sessions\1\BaseNamedObjects\GR55 Creates semaphore: \Sessions\1\BaseNamedObjects\GR56 Creates semaphore: \Sessions\1\BaseNamedObjects\GR57 Creates semaphore: \Sessions\1\BaseNamedObjects\GR58 Creates semaphore: \Sessions\1\BaseNamedObjects\GR59 Creates semaphore: \Sessions\1\BaseNamedObjects\GR60 \Sessions\1\BaseNamedObjects\GR61 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR62 Creates semaphore: \Sessions\1\BaseNamedObjects\GR63 \Sessions\1\BaseNamedObjects\GR64 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR66 Creates semaphore: \Sessions\1\BaseNamedObjects\GR67 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR68 Creates semaphore: \Sessions\1\BaseNamedObjects\GR69 \Sessions\1\BaseNamedObjects\GR70 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR71 \Sessions\1\BaseNamedObjects\GR72 Creates semaphore: \Sessions\1\BaseNamedObjects\GR73 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR74 \Sessions\1\BaseNamedObjects\GR75 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR76 Creates semaphore: \Sessions\1\BaseNamedObjects\GR77 Creates semaphore: \Sessions\1\BaseNamedObjects\GR78 Creates semaphore: \Sessions\1\BaseNamedObjects\GR79 \Sessions\1\BaseNamedObjects\GR80 Creates semaphore: \Sessions\1\BaseNamedObjects\GR81 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR82 \Sessions\1\BaseNamedObjects\GR83 Creates semaphore: \Sessions\1\BaseNamedObjects\GR84 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR85 \Sessions\1\BaseNamedObjects\GR86 Creates semaphore: \Sessions\1\BaseNamedObjects\GR87 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR88 $\verb|\Sessions|1\BaseNamedObjects|| GR89$ Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR90 Creates semaphore: \Sessions\1\BaseNamedObjects\GR91 Creates semaphore: \Sessions\1\BaseNamedObjects\GR92 Creates semaphore: \Sessions\1\BaseNamedObjects\GR93 \Sessions\1\BaseNamedObjects\GR94 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR95 Creates semaphore: \Sessions\1\BaseNamedObjects\GR96 Creates semaphore: \Sessions\1\BaseNamedObjects\GR97 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR99 Creates semaphore: \Sessions\1\BaseNamedObjects\GR100

Creates semaphore: \Sessions\1\BaseNamedObjects\INI-090ae821aa4e2bd4bddeb0cb6466b181.data0

File System Events

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

```
C:\Users\Admin\AppData\Roaming\GetRightToGo\090ae821aa4e2bd4bddeb0cb6466b181.data
 Creates
C:\Users\Admin\AppData\Roaming\GetRightToGo\090ae821aa4e2bd4bddeb0cb6466b181.data0
 Opens:
                         C:\Windows\System32
 Opens:
                         C:\Windows\Svstem32\sechost.dll
 Opens:
                         C:\windows\temp\090ae821aa4e2bd4bddeb0cb6466b181.exe.Local\
 Opens:
                         C:\Windows\winsxs\x86_microsoft.windows.common-
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
                         C:\windows\temp\oledlg.dll
 Opens:
 Opens:
                         C:\Windows\System32\oledlg.dll
 Opens:
                         C:\windows\temp\Secur32.dll
                         C:\Windows\System32\secur32.dll
 Opens:
 Opens:
                         C:\windows\temp\SSPICLI.DLL
 Opens:
                         C:\Windows\System32\sspicli.dll
 Opens:
                         C:\windows\temp\WINSPOOL.DRV
 Opens:
                         C:\Windows\System32\winspool.drv
 Opens:
                         C:\Windows\System32\imm32.dll
 Opens:
                         C:\Windows\WindowsShell.Manifest
 Opens:
                         C:\Windows\System32\uxtheme.dll
 Opens:
                         C:\windows\temp\090ae821aa4e2bd4bddeb0cb6466b181.exe.2.Manifest
                         C:\windows\temp\090ae821aa4e2bd4bddeb0cb6466b181.exe.3.Manifest
 Opens:
 Opens:
                         C:\windows\temp\090ae821aa4e2bd4bddeb0cb6466b181.exe.Config
 Opens:
                         C:\Windows\Temp\090ae821aa4e2bd4bddeb0cb6466b181.exe
                         C:\windows\temp\090ae821aa4e2bd4bddeb0cb6466b181.exe.1000.Manifest
 Opens:
 Opens:
                         C:\windows\temp\090ae821aa4e2bd4bddeb0cb6466b181ENU.dll
 Opens:
                         C:\windows\temp\090ae821aa4e2bd4bddeb0cb6466b181L0C.dll
 Opens:
                         C:\
 Opens:
                         C:\Users\Admin\AppData\Local
 Opens:
                         C:\Windows\System32\tzres.dll
                         C:\Windows\System32\en-US\tzres.dll.mui
 Opens:
 Opens:
                         C:\Windows\Fonts\tahoma.ttf
 Opens:
                         C:\windows\temp\dwmapi.dll
 Opens:
                         C:\Windows\System32\dwmapi.dll
 Opens:
                         C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens:
                         C:\Windows\System32\rpcss.dll
 Opens:
                         C:\windows\temp\CRYPTBASE.dll
 Opens:
                         C:\Windows\System32\cryptbase.dll
 Opens:
                         C:\Windows\Fonts\StaticCache.dat
                         {\tt C:\Windows\System32\shell32.dll}
 Opens:
 Opens:
                         C:\Users\Admin\Desktop
 Opens:
                         C:\Windows\System32\propsys.dll
                         C: \verb|\USers\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db|
 Opens:
 Opens:
                         C:\windows\temp\ntmarta.dll
 Opens:
                         C:\Windows\System32\ntmarta.dll
                         Opens:
4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000006.db
                         C:\Users\desktop.ini
 Opens:
 Opens:
                         C:\Users
 Opens:
                         C:\Users\Admin
 Opens:
                         C:\Users\Admin\Desktop\desktop.ini
 Opens:
                         C:\Windows\System32\en-US\setupapi.dll.mui
 Opens:
                         C:\Users\Admin\AppData\Roaming
                         C:\Users\Admin\AppData
 Opens:
                         C:\Users\Admin\AppData\Roaming\GetRightToGo
 Opens:
 Opens:
C:\Users\Admin\AppData\Roaming\GetRightToGo\090ae821aa4e2bd4bddeb0cb6466b181.data
                         C:\Windows\Temp
 Opens:
 Opens:
C:\Users\Admin\AppData\Roaming\GetRightToGo\090ae821aa4e2bd4bddeb0cb6466b181.data0
 Opens:
                         C:\Users\Admin\Desktop\Downloads\
 Opens:
                         C:\Users\Admin\Documents
 Opens:
                         C:\Users\Admin\Documents\desktop.ini
 Opens:
                         C:\Users\Public\Desktop
 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\090ae821aa4e2bd4bddeb0cb6466b181.data
C:\Users\Admin\AppData\Roaming\GetRightToGo\090ae821aa4e2bd4bddeb0cb6466b181.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\090ae821aa4e2bd4bddeb0cb6466b181.exe
 Reads from:
C:\Users\Admin\AppData\Roaming\GetRightToGo\090ae821aa4e2bd4bddeb0cb6466b181.data
 Reads from:
C:\Users\Admin\AppData\Roaming\GetRightToGo\090ae821aa4e2bd4bddeb0cb6466b181.data0
 Reads from:
                         C:\Users\Admin\Documents\desktop.ini
 Reads from:
                         C:\Users\Public\desktop.ini
```

Windows Registry Events

Creates key: HKCU\software\headlight Creates key: HKCU\software\headlight\getrighttogo HKCU\software\headlight\getrighttogo\sharedconfig Creates key: Creates key: HKCU\software\headlight\getrighttogo\customizedapps Opens key: HKLM\system\currentcontrolset\control\session manager Opens key: HKLM\system\currentcontrolset\control\terminal server Opens key: HKLM\system\currentcontrolset\control\safeboot\option HKLM\system\currentcontrolset\control\srp\gp\dll Opens kev: $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers$ Opens key: Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKCU\ HKCU\control panel\desktop\muicached\machinelanguageconfiguration Opens key: Opens key: HKLM\software\policies\microsoft\mui\settings Opens kev: HKCU\software\policies\microsoft\control panel\desktop Opens key: HKCU\control panel\desktop\languageconfiguration HKCU\control panel\desktop Opens key: Opens key: HKCU\control panel\desktop\muicached Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots Opens key: Opens key: HKLM\ Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics Opens key: HKLM\system\currentcontrolset\control\error message instrument\ HKLM\system\currentcontrolset\control\error message instrument Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32 Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ windows$ Opens key: Opens key: HKLM\software\microsoft\ole Opens key: HKLM\software\microsoft\ole\tracing HKLM\software\microsoft\oleaut Opens kev: Opens key: HKCU\software\classes\ Opens key: HKCU\software\classes\clsid Opens kev: HKCR\clsid Opens key: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\spaceshape}} \mbox{\tt policies\explorer} \mbox{\tt explorer} \mbox{\tt microsoft\windows\currentversion\spaceshape}} \mbox{\tt policies\explorer} \mbox{\tt explorer} \mbox{\tt$ Opens key: HKCU\software\microsoft\windows\currentversion\policies\network HKCU\software\microsoft\windows\currentversion\policies\comdlg32 Opens key: Opens key: HKLM\system\currentcontrolset\control\nls\customlocale Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale Opens key: HKLM\system\currentcontrolset\control\cmf\config Opens key: HKLM\software\microsoft\windows\windows error reporting\wmr Opens key: HKLM\system\currentcontrolset\control\computername Opens key: Opens key: HKLM\system\setup HKLM\system\currentcontrolset\control\nls\locale Opens key: Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts Opens key: HKLM\system\currentcontrolset\control\nls\language groups Opens key: HKLM\software\microsoft\ctf\compatibility\090ae821aa4e2bd4bddeb0cb6466b181.exe Opens key: $HKLM \setminus software \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be08 - b$ Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436} Opens key: HKLM\software\microsoft\ctf\ Opens key: HKLM\software\microsoft\ctf\knownclasses 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 nt\currentversion\languagepack\surrogatefallback HKLM\software\microsoft\windows Opens key: nt\currentversion\languagepack\surrogatefallback\ms shell dlg 2 HKLM\software\policies\microsoft\sqmclient\windows Opens key: Opens key: HKLM\software\microsoft\sqmclient\windows Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters Opens key: $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ appid_catalog$ Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\1dc99418 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries Opens key: Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000003

Opens key:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005 Opens kev:

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008 Opens kev:

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000011 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000012 Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000014 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000015 Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000017 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000018 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c 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\0000000000003 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\0000000000005 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000006

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

Opens key:

 $HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ applications \ 090 ae 821 aa 4e 2bd 4bd deb 0 cb 6466b 181. exemple \ descriptions \ desc$ Opens kev:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\fb4bfcc3a-db2c-424c-

b029-7fe99a87c641}

Opens kev:

b029-7fe99a87c641}\propertybag

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

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

Opens key:

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

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

folders Opens kev:

HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings Opens key:

08002b30309d}\shellfolder

HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder Opens kev:

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

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

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

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

Opens key: HKCU\software\microsoft\windows\currentversion\policies\nonenum $\label{thm:local_hammon} \parbox{$HKLM\software\microsoft\windows\currentversion\policies\nonenum} \parbox{$hkLM\software\microsoft\windows\currentversion\policies\nonenum} \parbox{$hkLM\software\microsoft\windows\currentversion\policies\nonenum} \parbox{$hkLM\software\microsoft\windows\currentversion\policies\nonenum} \parbox{$hkLM\software\microsoft\windows\currentversion\policies\nonenum} \parbox{$hkLM\software\microsoft\windows\currentversion\policies\nonenum} \parbox{$hkLM\software\windows\windows\currentversion\policies\nonenum\policies\nonenum\policies\nonenum\policies\nonenum\policies\policies\nonenum\policies\nonenum\policies\polici$ Opens kev:

Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume Opens kev:

11e3-b3bc-806e6f6e6963}\

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

Opens key: HKCR\drive\shellex\folderextensions

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

4442-804e-409d6c4515e9}

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

409d6c4515e9}

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

HKLM\software\microsoft\com3 Opens key:

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

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

b8dc300d9f9d}\treatas

 $HKCR \c1sid \f1f486a52-3cb1-48fd-8f50-b8dc300d9f9d \treatas$ Opens key: Opens key: HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\progid

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

b8dc300d9f9d}\inprocserver32

Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprochandler32

Opens key: $HKCR \c1sid \f1f486a52-3cb1-48fd-8f50-b8dc300d9f9d \c1f486a52-3cb1-48fd-8f50-b8dc300d9f9d \c1f$

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

b8dc300d9f9d}\inprochandler

Opens key: $HKCR \clsid \final 1f486a52-3cb1-48fd-8f50-b8dc300d9f9d \hinprochandler$ Opens key: HKLM\system\currentcontrolset\services\ldap Opens key:

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

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

Opens kev:

 $HKLM \label{lem:hklm} Software \mbox{\color=lem:hklm} in the constant \mbox{\color=lem:hklm} is the constant \mbox{\color=lem:hklm}. The constant \mbox{\color=lem:hklm} is the constant \mbox{\color=lem:hklm} in the color=lem:hklm, \mbox{\color=lem:hk$

Opens key:

HKCU\software\microsoft\windows\shell\associations\urlassociations\directory

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

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

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

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

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

HKCU\software\classes\allfilesystemobjects Opens key:

Opens key: HKCR\allfilesystemobjects

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

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

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

Opens key: HKCR\folder\docobject

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

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

Opens key: Opens kev: HKCR\directory\browseinplace

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

Opens key: HKCR\folder\browseinplace

 ${\tt HKCU \backslash software \backslash classes \backslash all file system objects \backslash browse in place}$ 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

HKCR\allfilesystemobjects\clsid Opens key:

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

Opens key: HKLM\software\microsoft\rpc

Opens key: HKLM\software\policies\microsoft\windows nt\rpc

Opens kev: HKCU\software

Opens key:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '{3}eb685db-65f9-4cf6-eps \ 'explorer' \ 'explorer'' \ 'explorer' \ 'explorer'' \$ a03a-e3ef65729f3d}

Opens key:

a03a-e3ef65729f3d}\propertybag

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

Opens key:

 $HKLM \ software \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1b3ea5dc-b587-4786-b5$ b4ef-bd1dc332aeae}\propertybag

Opens key:

11e3-b3bc-806e6f6e6963}\ Opens key: HKLM\software\policies\microsoft\windows\system Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\segoe ui Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46afadb4-6c85480369c7} Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46afadb4-6c85480369c7}\propertybag Opens key: HKCU\software\classes\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder HKCR\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder Opens key: 3f72-44a7-89c5-5595fe6b30ee}\shellfolder Opens key: afef-f87ef2e6ba25} Opens key: afef-f87ef2e6ba25}\propertybag HKLM\software\microsoft\windows\currentversion\explorer\user shell Opens key: folders Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\ms sans serif Oueries value: manager[cwdillegalindllsearch] Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat] Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled] Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled] ${\tt HKCU \backslash control\ panel \backslash desktop[preferreduilanguages]}$ Oueries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages] Queries value: Queries value: $HKLM \ software \ microsoft \ windows \ current version \ side by side [preferex ternal manifest]$ HKLM\system\currentcontrolset\control\nls\sorting\versions[] HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Queries value: HKLM\software\microsoft\windows Oueries value: nt\currentversion\gre_initialize[disablemetafiles] HKLM\software\microsoft\windows Oueries value: nt\currentversion\compatibility32[090ae821aa4e2bd4bddeb0cb6466b181] HKLM\software\microsoft\windows Oueries value: nt\currentversion\windows[loadappinit_dlls] Oueries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap] Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[en-us] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us] HKLM\system\currentcontrolset\control\nls\customlocale[en] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en] Queries value: HKLM\system\currentcontrolset\control\cmf\config[system] Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable] Oueries value: HKLM\system\currentcontrolset\control\computername\activecomputername[computername] Queries value: HKLM\system\setup[oobeinprogress] Oueries value: HKLM\system\setup[systemsetupinprogress] $HKLM \setminus system \setminus current control \setminus nls \setminus locale[00000409]$ Oueries value: HKLM\system\currentcontrolset\control\nls\language groups[1] Queries value: Queries value: Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable] HKLM\software\microsoft\ctf[enableanchorcontext] Queries value: HKLM\software\microsoft\windows Oueries value: nt\currentversion\languagepack\datastore_v1.0[disable] HKLM\software\microsoft\windows Oueries value: nt\currentversion\languagepack\datastore_v1.0[datafilepath] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane1] HKLM\software\microsoft\windows Oueries value: nt\currentversion\languagepack\surrogatefallback[plane2] HKLM\software\microsoft\windows Oueries value: nt\currentversion\languagepack\surrogatefallback[plane3]

Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane4] Oueries value: HKLM\software\microsoft\windows 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 Oueries value: 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]
                    HKLM\software\microsoft\windows
 Oueries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane11]|
                    HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane12]
                    HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane13]
                    HKLM\software\microsoft\windows
 Oueries value:
nt \verb|\currentversion| language pack \verb|\surrogatefallback[plane14]|
                    HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane15]
                     HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane16]
                    HKLM\software\microsoft\sqmclient\windows[ceipenable]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
 Oueries 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]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000005[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace \_catalog5 \ catalog\_entries \ 00000000001 [library path]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
 Queries 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:
Oueries value:
```

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ no mespace_catalog \ set no mespace_catalog_entries \ (000000000001[storesserviceclass in following the control set \ no mespace_catalog \ no$

Oueries value:

- 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[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]
 Oueries 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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
 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\00000000003[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 0000000000003 \ [version] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerinfo] Queries 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\0000000000004[displaystring]
 Oueries 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\000000000004[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace] Oueries 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring] Queries value:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 0000000000006 [providerid] \ Oueries \ value:$
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 000000000000006 [address family] \\ Queries \ value:$

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000006 [supported name space]]$ Oueries 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[storesserviceclassinfo] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[providerinfo] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount] Queries value: b029-7fe99a87c641}[category] Oueries value: b029-7fe99a87c641}[name] Queries value: b029-7fe99a87c641}[parentfolder] Oueries value: b029-7fe99a87c641}[description] Queries value: b029-7fe99a87c641}[relativepath] Oueries value: b029-7fe99a87c641}[parsingname]

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}[streamresourcetype]}$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} [local redirectonly]$

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} Learnest the sign of the second state of th$

Queries value:

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

Queries value:

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

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[publishexpandedpath]

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} current version \end{align* lem:hklmsoftware in the lateral properties of the l$

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} current version \verb| explorer folder descriptions $$\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}[folder type id]$$

Queries value:

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

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

folders[desktop]

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

08002b30309d}\shellfolder[attributes]

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

08002b30309d}\shellfolder[callforattributes]

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

08002b30309d}\shellfolder[restrictedattributes]

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

08002b30309d}\shellfolder[wantsfordisplay]

```
HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[hidefolderverbs]
   Oueries value:
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[usedrophandler]
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[wantsforparsing]
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
   Oueries value:
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforoverlay]
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[mapnetdriveverbs]
   Queries value:
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforinfotip]
   Queries value:
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideinwebview]
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[hideondesktopperuser]
   Queries value:
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsaliasednotifications]
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[wantsuniversaldelegate]
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[nofilefolderjunction]
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[pintonamespacetree]
                                                  HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hasnavigationenum]
   Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{20d04fe0-3aea-1069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8
08002b30309d}]
   Queries value:
11e3-b3bc-806e6f6e6963}[data]
   Oueries value:
11e3-b3bc-806e6f6e6963}[generation]
                                                 HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
   Oueries value:
409d6c4515e9}[drivemask]
                                                 HKLM\software\microsoft\com3[com+enabled]
   Queries value:
   Oueries value:
                                                 HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
                                                 HKCR\clsid\{1f486a52-3cb1-48fd-8f50-
   Queries value:
b8dc300d9f9d}\inprocserver32[inprocserver32]
                                                 HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[]
   Queries value:
                                                 HKCR\clsid\{1f486a52-3cb1-48fd-8f50-
   Oueries value:
b8dc300d9f9d}\inprocserver32[threadingmodel]
                                                 HKLM\software\microsoft\ole[maxsxshashcount]
   Queries value:
HKLM\svstem\currentcontrolset\control\lsa\accessproviders[martaextension]
                                                 HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
   Queries value:
                                                  HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
   Oueries value:
   Oueries value:
                                                 HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
   Queries value:
                                                 HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
   Queries value:
                                                  \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced[hidden]| \\ \end{tabular}
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
   Queries value:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{tabular} is a constant \cite{tabular}. The tabular \cite{tabular} is a constant \cite{tabular} is a co
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
   Queries value:
                                                  \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced| filter] \end{tabular}
   Oueries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus advanced [shows uper hidden]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
   Queries value:
Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
                                                 HKCR\directory[docobject]
   Oueries value:
   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: HKCR\directory[alwaysshowext]
Queries value: HKCR\directory[nevershowext]
Queries value: HKCR\folder[nevershowext]

Queries value: HKCR\allfilesystemobjects[nevershowext]

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

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

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}\category\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a$

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

Queries value:

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

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ ficon 1$

Queries value:

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

Queries value:

 $\label{lem:hklm} HKLM software \microsoft \windows \current version \explorer \folder descriptions \folder \cite{thm:hklm} a 03a-e3ef65729f3d \footnote{thm:hklm} software \microsoft \windows \current \cite{thm:hklm} software \microsoft \microsoft \cite{thm:hklm} software \microsoft \microsoft \cite{thm:hklm} software \microsoft \microsof$

Queries value:

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

Queries value:

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

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6a03a-e3ef65729f3d}[roamable]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

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

folders[appdata]

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \fill 1b3ea5dc-b587-4786-b4ef-bd1dc332aeae \current \curr$

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-

b4ef-bd1dc332aeae}[name]

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [parsing name]$

Oueries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ 'unidows \ 'current version \ 'explorer \ 'folder descriptions \ '\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [localized name]$

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{local-ham} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[stream]$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \mbox{$1b3ea5dc-b587-4786-b4ef-bd1dc332aeae} [attributes]$

Queries value:

 $HKLM \ software \ `microsoft \ 'current version \ 'explorer \ 'folder descriptions \ '\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [folder type id]$

Queries value:

 $HKLM \ software \ `microsoft \ 'current version \ 'explorer \ 'folder descriptions \ '\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [initfolder handler]$

Queries value:

 $HKCU \setminus software \\ microsoft \\ windows \\ current version \\ (explorer \\ mountpoints \\ (explorer \\ volume) \\ (explorer \\ (explorer \\ volume) \\ (explorer \\ (explorer \\ volume) \\$

Queries value:

 $\label{local-equation} HK\dot{C}U\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{69d250e3-6c18-11e3-b3bc-806e6f6e6963}\ [generation]$

Queries value: $\label{local-bsa-def-bd1} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \user shell folders \cite{local-bsa-def-bd1} dc332aeae \cite{local-bsa-def-bd1} \end{tabular}$

Oueries value:

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

 $\label{lem:policies} $$\operatorname{Queries value:}$ HKLM\software\policies\microsoft\windows\system[copyfilechunksize] $$\operatorname{HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount]} $$$

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

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\f(fdd39ad0-238f-46af-adb4-6c85480369c7)\category\cite{Abstraction}.$

Queries value:

 $HKLM \label{lem:hkkm} HKLM \label{lem:hkkm} HKLM \label{lem:hkkm} Software \mbox{ fdd39ad0-238f-46af-adb4-6c85480369c7} \ [name]$

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folder descriptions\f(fdd39ad0-238f-46af-adb4-6c85480369c7)\cite{Abstraction} folder and the second s$

Queries value:

 $\label{local-equation} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\f(fdd39ad0-238f-46af-adb4-6c85480369c7)\[description]$

Queries value:

 $\label{lem:hkkm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\fdd39ad0-238f-46af-adb4-6c85480369c7\[relative path]$

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ \ folder descriptions \ \ \ \ \ fdd 39 ad 0-238 f-46 af-46 af-46$ adb4-6c85480369c7}[parsingname]

adb4-6c85480369c7}[infotip]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ \ folder descriptions \ \ \ \ \ fdd 39 ad 0-238 f-46 af-46 af-46$ adb4-6c85480369c7}[localizedname]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46afadb4-6c85480369c7}[icon]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46afadb4-6c85480369c7}[security]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46afadb4-6c85480369c7}[streamresource]

Oueries value:

adb4-6c85480369c7}[streamresourcetype]

Queries value:

adb4-6c85480369c7}[localredirectonly]

Queries value:

adb4-6c85480369c7}[roamable]

Queries value:

adb4-6c85480369c7}[precreate]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46afadb4-6c85480369c7}[stream]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46afadb4-6c85480369c7}[publishexpandedpath]

Oueries value:

adb4-6c85480369c7}[attributes]

Queries value:

adb4-6c85480369c7}[foldertypeid]

Oueries value:

adb4-6c85480369c7}[initfolderhandler]

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

folders[personal]

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

5595fe6b30ee}\shellfolder[attributes]

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

5595fe6b30ee}\shellfolder[callforattributes]

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

5595fe6b30ee}\shellfolder[restrictedattributes]

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

5595fe6b30ee}\shellfolder[wantsfordisplay]

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

5595fe6b30ee}\shellfolder[hidefolderverbs]

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

5595fe6b30ee}\shellfolder[usedrophandler]

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

5595fe6b30ee}\shellfolder[wantsforparsing]

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

5595fe6b30ee}\shellfolder[wantsparsedisplayname]

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

5595fe6b30ee}\shellfolder[queryforoverlay]

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

5595fe6b30ee}\shellfolder[mapnetdriveverbs]

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

5595fe6b30ee}\shellfolder[queryforinfotip]

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

5595fe6b30ee}\shellfolder[hideinwebview]

HKCR\clsid\{59031a47-3f72-44a7-89c5-Oueries value: 5595fe6b30ee}\shellfolder[hideondesktopperuser]

Queries value:

HKCR\clsid\{59031a47-3f72-44a7-89c5-

5595fe6b30ee}\shellfolder[wantsaliasednotifications]

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

5595fe6b30ee}\shellfolder[wantsuniversaldelegate] Oueries value:

HKCR\clsid\{59031a47-3f72-44a7-89c5-

5595fe6b30ee}\shellfolder[nofilefolderjunction] Oueries value:

HKCR\clsid\{59031a47-3f72-44a7-89c5-

5595fe6b30ee}\shellfolder[pintonamespacetree]

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

5595fe6b30ee}\shellfolder[hasnavigationenum]

Oueries value:

 $HKLM \ software \ `microsoft\ `windows \ `current version \ policies \ `nonenum[\{59031a47-3f72-44a7-89c5-5595fe6b30ee\}]$

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} [description]$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{c4aa340d-f20f-4863-afef-f87ef2e6ba25\}[localized name]$

Queries value:

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} [security]$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{c4aa340d-f20f-4863-afef-f87ef2e6ba25\}[stream resource]$

Oueries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} [local redirectonly]$

Queries value:

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

Queries value:

 $HKLM \label{lem:hkkm} HKLM \label{lem:hkkm} HKLM \label{lem:hkkm} Software \mbox{$$m$icrosoft$ windows \current version \explorer \folder descriptions \cal{lem:hkkm} $$a340d-f20f-4863-afef-f87ef2e6ba25 \cal{lem:hkkm} $$p$ icrosoft \cal{lem:hkkm} $$a340d-f20f-4863-afef-f87ef2e6ba25 \cal{lem:hkkm} $$a340d-f20f-6864-afef-f87ef2e6ba25 \cal{le$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{c4aa340d-f20f-4863-afef-f87ef2e6ba25\}[stream]$

Oueries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-f20f-4863-afef-f87ef2e6ba25\}[publishexpandedpath]}$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{c4aa340d-f20f-4863-afef-f87ef2e6ba25\}[attributes]$

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{c4aa340d-f20f-4863-afef-f87ef2e6ba25\}[folder type id]$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{c4aa340d-f20f-4863-afef-f87ef2e6ba25\}[initfolder handler]$

 $\label{thm:linear} Queries \ value: \\ HKLM \ software \ microsoft \ windows \ current version \ version$

folders[common desktop]

Sets/Creates value:

HKCU\software\headlight\getrighttogo\customizedapps[090ae821aa4e2bd4bddeb0cb6466b181]

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]