Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 6, Task ID: 24

Task ID: 24 Risk Level: 5

Date Processed: 2016-04-28 12:46:42 (UTC)

Processing Time: 61.67 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\70c87e532c1ff4ae687b26c4224aa435.exe"

Sample ID: 6
Type: basic
Owner: admin

Label: 70c87e532c1ff4ae687b26c4224aa435

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

File Type: PE32:win32:gui File Size: 368256 bytes

MD5: 70c87e532c1ff4ae687b26c4224aa435

SHA256: 28b52897659cf99851f39f4f2c0c423f55a328ba2de1f3da894a85ba624b6e9b

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\70c87e532c1ff4ae687b26c4224aa435.exe

["C:\windows\temp\70c87e532c1ff4ae687b26c4224aa435.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex:

Creates semaphore:

Creates semaphore:

Creates semaphore: Creates semaphore:

Creates semaphore:

\Sessions\1\BaseNamedObjects\70c87e532c1ff4ae687b26c4224aa435.exeJAKbr7GE

Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0

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

Creates event: \KernelObjects\MaximumCommitCondition

Creates semaphore: \Sessions\1\BaseNamedObjects\INI-70c87e532c1ff4ae687b26c4224aa435.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

\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

> \Sessions\1\BaseNamedObjects\GR25 \Sessions\1\BaseNamedObjects\GR26

> \Sessions\1\BaseNamedObjects\GR27

\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: Creates semaphore: \Sessions\1\BaseNamedObjects\GR34 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 Creates semaphore: \Sessions\1\BaseNamedObjects\GR40 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: $\Sessions\1\BaseNamedObjects\GR65$ \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: Creates semaphore: \Sessions\1\BaseNamedObjects\GR84 Creates semaphore: \Sessions\1\BaseNamedObjects\GR85 \Sessions\1\BaseNamedObjects\GR86 Creates semaphore: \Sessions\1\BaseNamedObjects\GR87 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR88 Creates semaphore: \Sessions\1\BaseNamedObjects\GR89 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: $\verb|\Sessions|1\BaseNamedObjects|| GR98||$ Creates semaphore: \Sessions\1\BaseNamedObjects\GR99 Creates semaphore: \Sessions\1\BaseNamedObjects\GR100

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

 $\label{lem:condition} Creates: $C:\Users\land Admin\AppData\Roaming\GetRightToGo. $C:\Users\land Admin\AppData\Roaming\GetRightToGo. $$C:\Users\land Admin\AppData\Roaming\GetRightToGo. $$C:\Users\Admin\AppData\Roaming\GetRightToGo. $$C:\Users\Admin\AppData\Roaming\GetRightToGo. $$C:\Users\Admin\AppData\Roaming\GetRightToGo. $$C:\Users\Admin\AppData\Roaming\GetRightToGo. $$C:\Users\Admin\AppData\Roaming\GetRightToGo. $$C:\Users\Admin\AppData\Roaming\App$

Creates:

```
Creates
C:\Users\Admin\AppData\Roaming\GetRightToGo\70c87e532c1ff4ae687b26c4224aa435.data0
                                        C:\Windows\Prefetch\70C87E532C1FF4AE687B26C4224AA-15FA8DE2.pf
  Opens:
  Opens:
                                        C:\Windows
  Opens:
                                        C:\Windows\System32\wow64.dll
                                        C:\Windows\System32\wow64win.dll
  Opens:
  Opens:
                                        C:\Windows\System32\wow64cpu.dll
  Opens:
                                        C:\Windows\system32\wow64log.dll
  Opens:
                                        C:\Windows\SysWOW64
  Opens:
                                        C:\Windows\SysWOW64\sechost.dll
  Opens:
                                        C: \verb|\windows\temp\70c87e532c1ff4ae687b26c4224aa435.exe.Local\\| |
  Opens:
                                        C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
                                        C:\Windows\winsxs\x86_microsoft.windows.common-
  Opens:
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
  Opens:
                                       C:\windows\temp\oledlg.dll
  Opens:
                                        C:\Windows\SysWOW64\oledlg.dll
  Opens:
                                        C:\windows\temp\Secur32.dll
                                        C:\Windows\SysWOW64\secur32.dll
  Opens:
  Opens:
                                        C:\windows\temp\WINSPOOL.DRV
  Opens:
                                        C:\Windows\SysWOW64\winspool.drv
                                        C:\Windows\SysWOW64\imm32.dll
  Opens:
  Opens:
                                        C:\Windows\WindowsShell.Manifest
  Opens:
                                        C:\Windows\SysWOW64\uxtheme.dll
                                        C:\windows\temp\70c87e532c1ff4ae687b26c4224aa435.exe.2.Manifest
  Opens:
  Opens:
                                        C:\windows\temp\70c87e532c1ff4ae687b26c4224aa435.exe.3.Manifest
                                        C:\windows\temp\70c87e532c1ff4ae687b26c4224aa435.exe.Config
  Opens:
  Opens:
                                        C:\Windows\Temp\70c87e532c1ff4ae687b26c4224aa435.exe
  Opens:
                                        C:\windows\temp\70c87e532c1ff4ae687b26c4224aa435.exe.1000.Manifest
  Opens:
                                        C:\windows\temp\70c87e532c1ff4ae687b26c4224aa435ENU.dll
  Opens:
                                        C:\windows\temp\70c87e532c1ff4ae687b26c4224aa435L0C.dll
  Opens:
  Opens:
                                        C:\Users\Admin\AppData\Local
  Opens:
                                        C:\Windows\SysWOW64\tzres.dll
  Opens:
                                        C:\Windows\SysWOW64\en-US\tzres.dll.mui
  Opens:
                                        C:\Windows\Fonts\tahoma.ttf
  Opens:
                                        C:\windows\temp\dwmapi.dll
  Opens:
                                        C:\Windows\SysWOW64\dwmapi.dll
  Opens:
                                        C:\Windows\Globalization\Sorting\SortDefault.nls
                                        C:\Windows\SysWOW64\ole32.dll
  Opens:
  Opens:
                                        C:\Windows\SysWOW64\rpcss.dll
  Opens:
                                        C:\Windows\Fonts\StaticCache.dat
                                        C:\Windows\SysWOW64\shell32.dll
  Opens:
  Opens:
                                        C:\Users\Admin\Desktop
  Opens:
                                        C:\Windows\SysWOW64\propsys.dll
  Opens:
                                        \label{localMicrosoftWindows\Caches\cversions.1.db} C: \Users\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
  Opens:
                                        C:\windows\temp\ntmarta.dll
                                        C:\Windows\SysWOW64\ntmarta.dll
  Opens:
                                        \label{lem:condition} C: \label{lem:condition} C: \label{lem:condition} App Data \label{lem
  Opens:
4C77-AF34-C647E37CA0D9}.1.ver0x000000000000001.db
  Opens:
                                       C:\Users\desktop.ini
                                       C:\Windows\SysWOW64\en-US\setupapi.dll.mui
  Opens:
  Opens:
  Opens:
                                       C:\Users\Admin
                                        C:\Users\Admin\Desktop\desktop.ini
  Opens:
                                        C:\Users\Admin\AppData\Roaming
  Opens:
                                        C:\Users\Admin\AppData
  Opens:
                                        C:\Users\Admin\AppData\Roaming\GetRightToGo
  Opens:
  Opens:
C:\Users\Admin\AppData\Roaming\GetRightToGo\70c87e532c1ff4ae687b26c4224aa435.data
  Opens:
                                        C:\Windows\Temp
  Opens:
C:\Users\Admin\AppData\Roaming\GetRightToGo\70c87e532c1ff4ae687b26c4224aa435.data0
  Opens:
                                        C:\Users\Admin\Desktop\Downloads\
  Opens:
                                        C:\Windows\SysWOW64\en-US\user32.dll.mui
  Opens:
                                        C:\Users\Admin\Documents
                                       C:\Users\Admin\Documents\desktop.ini
  Opens:
  Opens:
                                        C:\Users\Public\Desktop
                                       C:\Users\Public\desktop.ini
  Opens:
  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\70c87e532c1ff4ae687b26c4224aa435.data
  Writes to:
C:\Users\Admin\AppData\Roaming\GetRightToGo\70c87e532c1ff4ae687b26c4224aa435.data0
                                        C:\Windows\Fonts\StaticCache.dat
  Reads from:
  Reads from:
                                        C:\Users\desktop.ini
  Reads from:
                                        C:\Users\Admin\Desktop\desktop.ini
  Reads from:
                                        C:\Windows\Temp\70c87e532c1ff4ae687b26c4224aa435.exe
  Reads from:
C:\Users\Admin\AppData\Roaming\GetRightToGo\70c87e532c1ff4ae687b26c4224aa435.data
```

C:\Users\Admin\AppData\Roaming\GetRightToGo\70c87e532c1ff4ae687b26c4224aa435.data

Reads from:

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

Creates key: HKCU\software\headlight

Creates key: HKCU\software\headlight\getrighttogo

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

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

options

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

Opens key: HKLM\software\microsoft\wow64

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

execution options

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

Opens key:

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

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

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

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

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

Opens key: HKCU\

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

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

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

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

Opens key:

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus side by side \setminus assembly storage roots$

Opens key: $\label{localization} \mbox{ HKLM} \mbox{ key: } \mbox{ HKLM} \mbox{ hklm} \mbox{ current controlset} \mbox{ control} \mbox{ hklm} \mbox{ system} \mbox{ current} \mbox{ current} \mbox{ control} \mbox{ hklm} \mbox{ system} \mbox{ current} \mbox{ current}$

Opens key: HKLM\

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

nt\currentversion\diagnostics

Opens key: $\label{thm:main} $$ HKLM\software\wow6432node\microsoft\windows nt\currentversion\gre_initialize $$$

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

nt\currentversion\compatibility32

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

compatibility

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

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

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

Opens key: HKCU\software\classes\

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

Opens key: HKCR\wow6432node\clsid

Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\policies\network
Opens key: HKCU\software\microsoft\windows\currentversion\policies\comdlg32

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

Opens key: HKLM\system\currentcontrolset\control\cmf\config

Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr

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

 $Opens~key: \\ HKLM \ system \ current control \ computer name \ active computer name \ act$

Opens key: HKLM\system\setup

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

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

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

Opens key:

 $\label{local-bound} HKLM \software \wow 6432 node \microsoft \ctf \compatibility \normaling \norm$

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

Opens key: HKLM\software\wow6432node\microsoft\ctf\knownclasses

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

Opens key: HKLM\software\microsoft\windows

 $\verb|nt\currentversion\languagepack\datastore_v1.0|$

Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\ms shell dlg 2 HKLM\software\policies\microsoft\sqmclient\windows Opens kev: Opens key: HKLM\software\microsoft\sqmclient\windows Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid catalog Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\0020f864 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000 Opens kev: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\00000028 Opens key: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog5 \ (catalog_entries) \ and \ (catalog). \\$ Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001 Opens kev: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000003 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000006 Opens kev: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer Opens key: Opens key: Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3a-b$ db2c-424c-b029-7fe99a87c641} Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{b4bfcc3a-bc1, b4bfcc3a-bc1, b4$ db2c-424c-b029-7fe99a87c641}\propertybag Opens key: HKCU\software\microsoft\windows\currentversion\explorer Opens key: Opens kev: $HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in follows folders$ Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ \ known foldersettings$ Opens kev: HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder Opens kev: 08002b30309d}\shellfolder Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ clsid \ \{20d04fe0-3aea-1069-4046fe0-3aea-4046fe0$

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

Opens kev:

a2d8-08002b30309d}\shellfolder

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

Opens key:

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

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

Opens key:

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

Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d4-8213-

11e3-a68e-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\software\wow6432node\policies\microsoft\windows\explorer

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

Opens key: HKLM\software\microsoft\com3

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

b8dc300d9f9d}

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

b8dc300d9f9d}\treatas

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

b8dc300d9f9d}\progid

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

b8dc300d9f9d}\progid

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

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler

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

b8dc300d9f9d}\inprochandler

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

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

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

 $Opens~key: \\ HKLM\software\wow6432node\microsoft\windows\currentversion\setup$

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

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

Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc

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

Opens key:

11e3-a68e-806e6f6e6963}\

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

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ shell registered applications \ writes sociations \ directory \ open with progids \ microsoft \ writes \ microsoft \ windows \ shell \ registered \ microsoft \ writes \ microsoft \ microsoft \ writes \ microsoft \ micr$

Opens key:

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

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

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

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

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

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

Opens key: HKCR\folder

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

Opens key: HKCR\folder\shellex\iconhandler

Opens key: HKCU\software\classes\allfilesystemobjects

Opens key: HKCR\allfilesystemobjects

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

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

Opens key: HKCR\directory\docobject

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

Opens key: HKCR\folder\docobject

 $Opens \ key: \\ \hspace{2.5cm} \mathsf{HKCU} \backslash \mathsf{software} \backslash \mathsf{classes} \backslash \mathsf{allfilesystemobjects} \backslash \mathsf{docobject}$

HKCR\allfilesystemobjects\docobject Opens key:

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

Opens key: HKCR\directory\browseinplace

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

Opens key: HKCR\folder\browseinplace

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

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

Opens key: HKCR\directory\clsid

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

HKCR\folder\clsid Opens key:

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

Opens key: HKCR\allfilesystemobjects\clsid

Opens key: HKCU\software

Opens key:

65f9-4cf6-a03a-e3ef65729f3d}

Opens key:

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

b587-4786-b4ef-bd1dc332aeae}

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

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

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

HKLM\software\microsoft\windows Opens kev: nt\currentversion\languagepack\surrogatefallback\segoe ui

Opens key:

 $HKLM \label{lem:hklm} White the latest and the la$ 238f-46af-adb4-6c85480369c7}

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}\propertybag

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

5595fe6b30ee}\shellfolder

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

5595fe6b30ee}\shellfolder

 $\label{thm:local-continuous} HKCU \software \microsoft \windows \current version \explorer \clsid \cline{100} \c$ Opens key:

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

Opens kev:

89c5-5595fe6b30ee}\shellfolder

Opens key:

f20f-4863-afef-f87ef2e6ba25}

Opens kev:

f20f-4863-afef-f87ef2e6ba25}\propertybag

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

shell folders

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

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

options[disableusermodecallbackfilter]

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

manager[cwdillegalindllsearch]

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

 $HKLM \verb|\software| policies \verb|\microsoft| windows \verb|\safer| code identifiers[transparentenabled]|$ HKLM\system\currentcontrolset\control\nls\customlocale[empty] Oueries value:

Oueries value:

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

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

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

us[alternatecodepage]

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

 $\label{local-control} \mbox{ HKCU\control panel\desktop\muicached[machinepreferreduilanguages]} \\$ Queries value:

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]

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

Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]

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

HKLM\software\wow6432node\microsoft\windows Oueries value: nt\currentversion\compatibility32[70c87e532c1ff4ae687b26c4224aa435] Oueries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\windows[loadappinit_dlls]

Oueries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap] Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]

```
HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Oueries value:
  Oueries value:
                                 HKLM\svstem\currentcontrolset\control\nls\extendedlocale[en-usl
  Oueries value:
                                 HKLM\system\currentcontrolset\control\nls\customlocale[en]
  Queries value:
                                 HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
  Oueries value:
                                 HKLM\svstem\currentcontrolset\control\cmf\config[svstem]
  Queries value:
                                 reporting\wmr[disable]
  Oueries value:
HKLM\system\currentcontrolset\control\computername[activecomputername]
  Queries value:
                                 HKLM\system\setup[oobeinprogress]
                                 HKLM\system\setup[systemsetupinprogress]
  Oueries value:
  Queries value:
                                 HKLM \setminus system \setminus current control \setminus nls \setminus locale[00000409]
  Oueries value:
                                 HKLM\system\currentcontrolset\control\nls\language groups[1]
                                 HKLM \setminus software \setminus microsoft \setminus ctf \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07 - be07 - be18 - be
  Oueries value:
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
  Queries value:
                                 HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
  Queries value:
                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
  Queries value:
                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
                                 HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane1]
                                 HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane2]
                                 HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane3]
                                 HKLM\software\microsoft\windows
  Queries value:
\verb|nt\currentversion\language| pack\surrogatefallback[plane4]|
  Oueries value:
                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
                                 HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane6]
                                 HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane7]
  Oueries value:
                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
  Oueries value:
                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
                                 HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane10]
  Queries value:
                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
                                 HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane12]
                                 HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane13]
  Queries value:
                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
  Oueries value:
                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
                                 HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane16]
  Queries value:
                                 HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus 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]
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000004[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000005[packedcatalogitem]
  Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000008[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
  Oueries value:
```

Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace_catalog 5 [serial_access_num]$

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]
 Oueries 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\000000000001[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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\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\000000000002[displaystring]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog \ solves \ value:$
- 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]
 Queries 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerinfo]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 00000000000004 [library path] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 0000000000004 [storesservice class info] \\ Oueries \ value:$
- 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:
- $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace_catalog \catalog_entries \namespace_catalog \catalog_entries \catalog \catalog_entries \catalog \catalog_entries \catalog \cat$

```
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000005 \ [address family]
  Oueries value:
```

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

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus names pace_catalog \\ \setminus catalog_entries \setminus 0000000000005 [enabled]$ Queries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_\catalog_entries\00000000005[storesserviceclassinfo] Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap services \setminus mame space_catalog \\ \setminus catalog_entries \setminus 0000000000005[provider in fo]$ Queries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring] Queries value:

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

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

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000006 [supported name space]]$ Queries value:

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

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

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog5 \ catalog_entries \ 10000000000006 \ [storesservice classinfo]$ Queries value:

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

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ policies \ \ explorer [no properties my computer]$ Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ policies \ explorer \ [no proper ties recyclebin]$

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

Queries value:

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

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

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

```
db2c-424c-b029-7fe99a87c641}[roamable]
   Oueries value:
db2c-424c-b029-7fe99a87c641}[precreate]
db2c-424c-b029-7fe99a87c641}[stream]
   Oueries value:
db2c-424c-b029-7fe99a87c641}[publishexpandedpath]
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}[attributes]
   Queries value:
db2c-424c-b029-7fe99a87c641}[foldertypeid]
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{b4bfcc3a-bc1, b4bfcc3a-bc2, b4
db2c-424c-b029-7fe99a87c641}[initfolderhandler]
                                            HKCU\software\microsoft\windows\currentversion\explorer\user shell
   Queries value:
folders[desktop]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[attributes]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[callforattributes]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[restrictedattributes]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[wantsfordisplay]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[hidefolderverbs]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[usedrophandler]
   Oueries value:
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsforparsing]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[queryforoverlay]
   Queries value:
                                            08002b30309d}\shellfolder[mapnetdriveverbs]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[queryforinfotip]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[hideinwebview]
   Queries value:
                                            08002b30309d}\shellfolder[hideondesktopperuser]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
                                            Oueries value:
08002b30309d}\shellfolder[wantsuniversaldelegate]
   Queries value:
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[nofilefolderjunction]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[pintonamespacetree]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[hasnavigationenum]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}1
   Oueries value:
11e3-a68e-806e6f6e6963}[data]
   Queries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ 13-623 \ del{eq:microsoft}.
11e3-a68e-806e6f6e6963}[generation]
   Queries value:
                                            HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
                                            HKLM\software\microsoft\com3[com+enabled]
   Oueries value:
                                            HKCR \setminus wow6432 \\ node \\ clsid \\ \{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\}[]
   Queries value:
                                            HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
   Oueries value:
b8dc300d9f9d}\inprocserver32[inprocserver32]
   Queries value:
                                            HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[]
   Oueries value:
                                            HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[threadingmodel]
   Oueries value:
                                            HKLM\software\microsoft\ole[maxsxshashcount]
   Oueries value:
HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
   Queries value:
                                            HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
   Oueries value:
                                            HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
   Queries value:
                                            HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
```

Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate] Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath] HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath] Oueries value: Queries value: HKLM\software\microsoft\rpc[maxrpcsize] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview] Oueries value:

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

Oueries value:

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

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-

11e3-a68e-806e6f6e6963}[data]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-

11e3-a68e-806e6f6e6963}[generation]

Oueries value:

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

Queries value:

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

HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden] Oueries value:

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $HKCU \ software \ `microsoft \ `windows \ `current version \ `explorer \ `advanced \ [mapnet drvbtn]" \ in the context of th$

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

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

Queries value:

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

Oueries value:

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

Oueries value: HKCR\directory[docobject]

Oueries value: HKCR\folder[docobiect]

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

Queries value: HKCR\allfilesystemobjects[browseinplace]

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

 ${\tt HKCR\ left} lesystemobjects [is short cut]$ Oueries value:

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

HKCR\allfilesystemobjects[nevershowext] Queries value:

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

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

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

Queries value:

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

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

Queries value:

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

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{3eb685db-10explorer\} \ folder \ before \ folder \ before \ folder \ folder \ before \ folder \ fol$ 65f9-4cf6-a03a-e3ef65729f3d}[parsingname]

Oueries value:

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

Queries value

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ user shell$

folders[appdata]

Queries value:

Queries value:

Queries value:

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

Queries value:

 $\label{thm:hklm} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fill\\ b587-4786-b4ef-bd1dc332aeae\fill\\ [description]$

Oueries value:

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

Queries value:

Queries value:

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

Queries value:

 $\label{localized} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fill 1b3ea5dc-b587-4786-b4ef-bd1dc332 aeae \cite{localized} \cite{localized} \end{subarray} \label{localized}$

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[icon]

Queries value

Queries value:

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

Queries value

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

Queries value:

Oueries value:

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

Oueries value

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

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}]

Queries value:

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

Queries value: HKLM\software\policies\microsoft\windows\system[copyfilechunksize]
Queries value: HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount]
Queries value: HKCU\software\headlight\getrighttogo\sharedconfig[debug]

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries 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:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} \ finfotip \ label{eq:hklm}$

Queries value:

 $\label{localized} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f(fdd39ad0-238f-46af-adb4-6c85480369c7)\[localized name]$

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-observation} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f(fdd39ad0-238f-46af-adb4-6c85480369c7)\[streamresource]$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

```
238f-46af-adb4-6c85480369c7}[foldertypeid]
      Oueries value:
238f-46af-adb4-6c85480369c7}[initfolderhandler]
                                                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
      Queries value:
 folders[personal]
                                                                                 HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
      Oueries value:
5595fe6b30ee}\shellfolder[attributes]
      Oueries value:
                                                                                  HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder[callforattributes]
                                                                                 HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
      Queries value:
 5595fe6b30ee}\shellfolder[restrictedattributes]
     Oueries value:
                                                                                 HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder[wantsfordisplay]
                                                                                  HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
      Queries value:
5595fe6b30ee}\shellfolder[hidefolderverbs]
                                                                                 HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
      Queries value:
 5595fe6b30ee}\shellfolder[usedrophandler]
                                                                                 HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
      Queries value:
5595fe6b30ee}\shellfolder[wantsforparsing]
                                                                                  HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
      Queries value:
5595fe6b30ee}\shellfolder[wantsparsedisplayname]
                                                                                  HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
 5595fe6b30ee}\shellfolder[queryforoverlay]
                                                                                 HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
      Queries value:
5595fe6b30ee}\shellfolder[mapnetdriveverbs]
                                                                                 HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
      Queries value:
5595fe6b30ee}\shellfolder[queryforinfotip]
                                                                                 HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
      Queries value:
 5595fe6b30ee}\shellfolder[hideinwebview]
                                                                                 HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
      Queries value:
 5595fe6b30ee}\shellfolder[hideondesktopperuser]
      Queries value:
                                                                                  HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder[wantsaliasednotifications]
                                                                                 HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
      Queries value:
 5595fe6b30ee}\shellfolder[wantsuniversaldelegate]
      Queries value:
                                                                                 HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
 5595fe6b30ee}\shellfolder[nofilefolderjunction]
                                                                                 HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
      Queries value:
5595fe6b30ee}\shellfolder[pintonamespacetree]
                                                                                 HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
      Queries value:
 5595fe6b30ee}\shellfolder[hasnavigationenum]
      Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{59031a47-3f72-44a7-89c5-
5595fe6b30ee}1
      Queries value:
HKLM \label{lem:hklm} White the latest and the la
f20f-4863-afef-f87ef2e6ba25}[category]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}[name]
      Queries value:
HKLM \label{lem:hklm} White the latest and the la
f20f-4863-afef-f87ef2e6ba25}[parentfolder]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}[description]
      Oueries value:
f20f-4863-afef-f87ef2e6ba25}[relativepath]
      Queries value:
HKLM \label{lem:hklm} White the latest and the la
f20f-4863-afef-f87ef2e6ba25}[parsingname]
      Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{c4aa340d-microsoft \ windows \ current \ version \ \ \}
 f20f-4863-afef-f87ef2e6ba25}[infotip]
      Queries value:
f20f-4863-afef-f87ef2e6ba25}[localizedname]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
 f20f-4863-afef-f87ef2e6ba25}[icon]
      Queries value:
HKLM \label{lem:hklm} White the latest and the la
f20f-4863-afef-f87ef2e6ba25}[security]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
 f20f-4863-afef-f87ef2e6ba25}[streamresource]
      Oueries value:
HKLM \label{lem:hklm} White the latest and the la
```

f20f-4863-afef-f87ef2e6ba25}[streamresourcetype]

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:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value

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

Queries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\currentversion\explorer\folder descriptions\currentversion\explorer\folder descriptions\currentversion\explorer\folder descriptions\currentversion\explorer\fold$

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations] Sets/Creates value:$

HKCU\software\headlight\getrighttogo\customizedapps[70c87e532c1ff4ae687b26c4224aa435]

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]