Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 170, Task ID: 681

Task ID: 681 Risk Level: 5

Date Processed: 2016-04-28 13:05:39 (UTC)

Processing Time: 61.21 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\c1a5167faf749c474083cf838ee771c6.exe"

Sample ID: 170 Type: basic Owner: admin

Label: c1a5167faf749c474083cf838ee771c6

Date Added: 2016-04-28 12:45:07 (UTC)

File Type: PE32:win32:gui File Size: 968288 bytes

MD5: c1a5167faf749c474083cf838ee771c6

SHA256: 78154134c9c621850328f4826bcd314f3852c60ff0e1b4ffd3b45a9f84adcd9c

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\c1a5167faf749c474083cf838ee771c6.exe

["C:\windows\temp\c1a5167faf749c474083cf838ee771c6.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\c1a5167faf749c474083cf838ee771c6.exeHXvucXBa

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-c1a5167faf749c474083cf838ee771c6.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 Creates semaphore: \Sessions\1\BaseNamedObjects\GR4 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 $\verb|\Sessions|1| BaseNamedObjects| GR13|$ Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR14 Creates semaphore: \Sessions\1\BaseNamedObjects\GR15 \Sessions\1\BaseNamedObjects\GR16 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR17 Creates semaphore: \Sessions\1\BaseNamedObjects\GR18 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 Creates semaphore: \Sessions\1\BaseNamedObjects\GR32 \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 \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: $\Sessions\1\BaseNamedObjects\GR65$ \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 Creates semaphore: \Sessions\1\BaseNamedObjects\INI-c1a5167faf749c474083cf838ee771c6.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\c1a5167faf749c474083cf838ee771c6.data
C:\Users\Admin\AppData\Roaming\GetRightToGo\c1a5167faf749c474083cf838ee771c6.data0
                                             C:\Windows\Prefetch\C1A5167FAF749C474083CF838EE77-7A9220C8.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:\windows\temp\c1a5167faf749c474083cf838ee771c6.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-
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
   Opens:
                                             C:\Windows\SysWOW64\imm32.dll
   Opens:
                                             C:\Windows\WindowsShell.Manifest
   Opens:
                                             C:\Windows\SysWOW64\uxtheme.dll
                                             C:\windows\temp\c1a5167faf749c474083cf838ee771c6.exe.2.Manifest
   Opens:
   Opens:
                                             C:\windows\temp\c1a5167faf749c474083cf838ee771c6.exe.3.Manifest
   Opens:
                                             C:\windows\temp\c1a5167faf749c474083cf838ee771c6.exe.Config
   Opens:
                                             C:\Windows\Temp\c1a5167faf749c474083cf838ee771c6.exe
   Opens:
                                             C:\windows\temp\c1a5167faf749c474083cf838ee771c6.exe.1000.Manifest
   Opens:
                                             C:\windows\temp\c1a5167faf749c474083cf838ee771c6ENU.dll
   Opens:
                                             C:\windows\temp\c1a5167faf749c474083cf838ee771c6L0C.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{local-Microsoft-Windows-Caches-Constant} C: \Users \land Admin \land App Data \land Local \land Microsoft \land Windows \land Caches \land 
   Opens:
                                             C:\windows\temp\ntmarta.dll
                                             C:\Windows\SysWOW64\ntmarta.dll
   Opens:
                                             Opens:
4C77-AF34-C647E37CA0D9}.1.ver0x000000000000001.db
                                             C:\Users\desktop.ini
   Opens:
                                             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\c1a5167faf749c474083cf838ee771c6.data
   Opens:
                                             C:\Windows\Temp
   Opens:
C:\Users\Admin\AppData\Roaming\GetRightToGo\c1a5167faf749c474083cf838ee771c6.data0
                                             C:\Users\Admin\Desktop\Downloads\
   Opens:
   Opens:
                                             C:\Users\Admin\Documents
   Opens:
                                             C:\Users\Admin\Documents\desktop.ini
                                             C:\Users\Public\Desktop
   Opens:
   Opens:
                                             C:\Users\Public\desktop.ini
                                             C:\Users\Public
   Opens:
                                             C:\Users\Public\Desktop\desktop.ini
   Opens:
   Opens:
                                             C:\Windows\Fonts\sserife.fon
   Writes to:
C:\Users\Admin\AppData\Roaming\GetRightToGo\c1a5167faf749c474083cf838ee771c6.data
C:\Users\Admin\AppData\Roaming\GetRightToGo\c1a5167faf749c474083cf838ee771c6.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\c1a5167faf749c474083cf838ee771c6.exe
C:\Users\Admin\AppData\Roaming\GetRightToGo\c1a5167faf749c474083cf838ee771c6.data
```

Reads from:

 $C: \verb|Vsers| Admin| AppData| Roaming | GetRightToGo| c1a5167faf749c474083cf838ee771c6.data0| data0| data0|$

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

Windows Registry Events

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:

 $HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers$

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:

 $HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hkklm} \label{lem:hkklm} \label{lem:hkklm} HKLM \label{lem:hkklm} \label{lkklm} \labell} \label{lkklm} \labell{lkklm} \labell{lkklm} \labell{lkklm} \labell{lkklm} \labell} \labell{lkklm} \labell{lkklm} \labell{lk$

Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions

Opens key: HKLM\

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

nt\currentversion\diagnostics

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

nt\currentversion\gre_initialize

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

 $\verb|nt\currentversion\compatibility32| \\$

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

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

Opens key: HKLM\system\setup

 $Opens \; key: \\ \qquad \qquad \text{HKLM} \\ system \\ \text{current control } \\ \text{nls } \\ \text{locale}$

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

Opens key:

 $\label{language} Of 16 + 0x00000000 \ 0001 \ be 3-ed 56-483 \ d-a 2e 2-a ea e 25577436 \ Opens \ key: \ HKLM \ microsoft \ tip \ 0000897 \ b-83 \ d-4b96-be 07-0f 58b 01c 4a 4 \ \ language \ profile \ 0x00000000 \ 0001 \ be 3-ed 56-483 \ d-a 2e 2-a ea e 25577436 \ d-a 2e 2-a e 2 e$

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

nt\currentversion\languagepack\datastore_v1.0

Opens key: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback HKLM\software\microsoft\windows Opens kev: nt\currentversion\languagepack\surrogatefallback\ms shell dlg 2 Opens key: HKLM\software\policies\microsoft\sqmclient\windows HKLM\software\microsoft\sqmclient\windows Opens key: Opens key: $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters$ Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\0cb22320 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005 Opens key: $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap col_catalog 9 \setminus catalog_entries$ Opens key: Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003 Opens key: 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\000000000007 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008 Opens key: Opens key: $HKLM \land system \land current control set \land services \land winsock 2 \land parameters \land protocol_catalog9 \land catalog_entries \land 000000000010 \land parameters \land protocol_catalog9 \land catalog_entries \land 0000000000010 \land parameters \land para$ HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer Opens kev: Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions Opens key: db2c-424c-b029-7fe99a87c641} Opens kev: db2c-424c-b029-7fe99a87c641}\propertybag HKCU\software\microsoft\windows\currentversion\explorer Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders Opens kev: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings Opens key: HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder Opens key: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-

 $HKCU \setminus software \setminus icrosoft \setminus windows \setminus current version \setminus explorer \setminus (20d04feo-block) + (20d04feo-block) +$

08002b30309d}\shellfolder

a2d8-08002b30309d}\shellfolder

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

Opens key:

Opens key:

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 kev:

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

Opens kev:

11e3-a68e-806e6f6e6963}\

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

Opens key: HKCR\drive\shellex\folderextensions

Opens key: $HKCU \setminus software \land classes \land drive \land shell ex \land folder extensions \land \{fbeb8a05-beee-beed extensions \land \{fbeb8a05-beed extensions \} \}$

4442-804e-409d6c4515e9}

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

409d6c4515e9}

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

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

b8dc300d9f9d}\treatas

Opens key: $HKCR \setminus wow6432 node \\ clsid \\ \{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\} \\ \\ \\ treatas$ Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{1f486a52 - 3cb1 - 48fd - 8f50 - 48fd - 8f50$

b8dc300d9f9d}\progid

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

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

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler

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

b8dc300d9f9d}\inprochandler

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

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

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

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

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

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

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

Opens kev: Opens key:

 $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\advanced}} \\$

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

Opens key: HKCR\folder

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

Opens key: HKCR\folder\shellex\iconhandler

 ${\tt HKCU \backslash software \backslash classes \backslash all file system objects}$ Opens key:

Opens key: HKCR\allfilesvstemobjects

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

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

Opens kev: HKCR\directory\docobject

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

HKCR\folder\docobject Opens key:

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

Opens key: HKCR\allfilesystemobjects\docobject

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

Opens kev: HKCR\directory\browseinplace

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

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

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

Opens key:

HKCU\software\classes\folder\clsid

Opens key: HKCR\folder\clsid

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

Opens key: HKCR\allfilesystemobjects\clsid

Opens key:

11e3-a68e-806e6f6e6963}\

Opens key: HKCU\software

Opens key:

65f9-4cf6-a03a-e3ef65729f3d}

Opens key:

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

b587-4786-b4ef-bd1dc332aeae}

Opens kev:

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

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

238f-46af-adb4-6c85480369c7}

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

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

5595fe6b30ee}\shellfolder

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

5595fe6b30ee}\shellfolder

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{59031a47-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{59031a47-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{59031a47-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{59031a47-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{59031a47-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{59031a47-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{59031a47-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{59031a47-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{59031a47-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{59031a47-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{59031a47-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{59031a47-microsoft \setminus explorer \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus explorer \setminus clsid \setminus explorer \setminus clsid$ Opens key:

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

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{59031a47-3f72-44a7-

89c5-5595fe6b30ee}\shellfolder

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{c4aa340d-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{c4aa340d-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{c4aa340d-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{c4aa340d-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{c4aa340d-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{c4aa340d-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{c4aa340d-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{c4aa340d-microsoft \setminus windows \setminus current \\ descriptions \setminus \{c4aa340d-m$

f20f-4863-afef-f87ef2e6ba25}

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-

f20f-4863-afef-f87ef2e6ba25}\propertybag

Opens kev:

shell folders

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

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

options[disableusermodecallbackfilter]

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

manager[cwdillegalindllsearch]

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

Queries value:

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

Oueries value:

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

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

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

us[alternatecodepage]

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

HKCU\control panel\desktop\muicached[machinepreferreduilanguages] Oueries value:

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [prefer external manifest] \ description \ descriptio$

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

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

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

Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[c1a5167faf749c474083cf838ee771c6] HKLM\software\wow6432node\microsoft\windows Oueries value:

nt\currentversion\windows[loadappinit_dlls]

Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap] HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]

```
Oueries value:
                                    HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Oueries value:
                                    HKLM\system\currentcontrolset\control\nls\customlocale[en]
  Oueries value:
                                    HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
  Queries value:
                                    HKLM\system\currentcontrolset\control\cmf\config[system]
  Oueries value:
                                    HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:
                                    HKLM\system\setup[oobeinprogress]
  Queries value:
                                    HKLM\system\setup[systemsetupinprogress]
                                    HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Oueries value:
  Queries value:
                                    HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:
                                    HKLM \setminus software \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07 - be07 - be18 - b
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
                                    HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
  Queries value:
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
                                    HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
                                    HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane2]
                                    HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane3]
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
                                    HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane5]
                                    HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane6]
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
                                    HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane8]
                                    HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane9]
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
                                    HKLM\software\microsoft\windows
  Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane11]|
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
                                    HKLM\software\microsoft\windows
  Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane14]|
  Queries value:
                                    HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback[plane15]|
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
                                    HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Oueries value:
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Oueries 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:
Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 0000000000003 \ [packed catalog item]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000004[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[packedcatalogitem]
```

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]

Queries value:

Oueries value:

Queries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 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\00000000001[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
 Queries 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\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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
- 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\00000000003[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\00000000003[enabled]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 0000000000003 \ [version] \ Oueries \ value:$
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries \ 000000000003 \ [storesservice class info] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
- 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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[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]
- $\label{lem:hklm} \begin{tabular}{ll} HKLM\system \current control set \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \namespace_catalog 5 \catalog_entries \namespace] \end{tabular} \begin{tabular}{ll} Queries value: \namespace_catalog 5 \catalog_entries \namespace_catalog$
- 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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerid]
 Oueries value:

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\000000000005[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\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
 Oueries value:

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

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

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

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo] Oueries value:

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

Queries value:

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

Queries value:

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

Queries value.

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

Queries value:

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

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

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

 $\label{thm:microsoftwindows} HKLM software \noindows \$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma[]{\colorer-folderdescriptions}\gamma[]{\colorer-folderdescription$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\begin{tabular}{l} \begin{tabular}{l} \be$

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

Queries value:

Queries value:

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

Queries value:

```
db2c-424c-b029-7fe99a87c641}[roamable]
   Oueries value:
db2c-424c-b029-7fe99a87c641}[precreate]
   Oueries value:
db2c-424c-b029-7fe99a87c641}[stream]
   Oueries value:
db2c-424c-b029-7fe99a87c641}[publishexpandedpath]
   Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b
db2c-424c-b029-7fe99a87c641}[attributes]
   Oueries value:
db2c-424c-b029-7fe99a87c641}[foldertypeid]
   Oueries value:
db2c-424c-b029-7fe99a87c641}[initfolderhandler]
                                             HKCU\software\microsoft\windows\currentversion\explorer\user shell
   Oueries value:
folders[desktop]
   Queries value:
                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[callforattributes]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[restrictedattributes]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[wantsfordisplay]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[hidefolderverbs]
   Queries value:
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[usedrophandler]
   Queries value:
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsforparsing]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
                                            Oueries value:
08002b30309d}\shellfolder[queryforoverlay]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[mapnetdriveverbs]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[quervforinfotip]
   Queries value:
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideinwebview]
                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[hideondesktopperuser]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
   Queries value:
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsuniversaldelegate]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[nofilefolderjunction]
   Queries value:
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[pintonamespacetree]
   Queries value:
                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hasnavigationenum]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}]
  Queries value:
\label{prop:local-hammon} HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ \{8063a3d4-8213-42d4, \mountpoints 2 \cpc \volume \ \{8063a3d4-8213-42d4, \mountpoints 2 \cpc \volume \ \} \ \mountpoints 
11e3-a68e-806e6f6e6963}[data]
   Oueries value:
11e3-a68e-806e6f6e6963}[generation]
                                             HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
  Queries value:
409d6c4515e9}[drivemask]
   Queries value:
                                             HKLM\software\microsoft\com3[com+enabled]
                                             HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
   Oueries value:
   Queries value:
                                             HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[inprocserver32]
                                            HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
   Oueries value:
b8dc300d9f9d}\inprocserver32[]
   Queries value:
                                            HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[threadingmodel]
   Queries value:
                                            HKLM\software\microsoft\ole[maxsxshashcount]
   Oueries value:
HKLM \verb|\system| current control \verb|\sa| access providers [marta extension]|
   Oueries value:
                                            HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
   Queries value:
                                             HKLM \setminus system \setminus current control set \setminus services \setminus ldap [use old host resolution order]
   Oueries value:
                                             HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
```

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

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

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\setup[sourcepath] $HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus windows \setminus current version [device path]$ Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

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

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

Oueries value: Oueries value:

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

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

Oueries value:

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

Queries value:

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

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

Oueries value:

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]

Queries value:

 $HKCU \ software \ \verb|microsoft| windows \ \verb|currentversion| explorer \ \verb|advanced[separate process]|$

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

Oueries value:

Queries value:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \current version \explorer \advanced [iconsonly] \end{tabular}$

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

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

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

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

HKCR\allfilesystemobjects[browseinplace] Oueries value:

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

Oueries value: HKCR\allfilesvstemobjects[isshortcut]

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

Queries value: HKCR\allfilesystemobjects[nevershowext]

Oueries value:

11e3-a68e-806e6f6e6963}[data]

11e3-a68e-806e6f6e6963}[generation]

HKCU\software\headlight\getrighttogo\sharedconfig[useloadimage] Queries value: $\label{lem:headlight} HKCU \ software \ head light \ getright to go \ shared config \ [doxpthemes]$ Oueries value:

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value

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

Oueries value

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

Oueries value:

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

Oueries value

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

Oueries value:

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

Oueries value:

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

Oueries value

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

Oueries value:

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

Queries value:

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

folders[appdata]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\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\folderdescription\currentversion\explorer\folderdescription\currentversion\explorer\folderdescription\currentversion\explorer\folderdescription\currentversion\explorer\folderdescription\currentversion\explorer\currentversion\$

Queries value:

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

Queries value:

 $\label{thm:local-basis} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\f(1b3ea5dc-b587-4786-b4ef-bd1dc332 aeae)\currentversion\explorer\folder descriptions\f(1b3ea5dc-b587-4786-b4ef-bd1dc332 aeae)\currentversion\explorer\curre$

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{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:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{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:

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

Oueries value:

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

Oueries value

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

Queries value:

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

Queries value:

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

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

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

Oueries value:

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

Queries value: HKLM\software\policies\microsoft\windows\system[copyfilechunksize]
Queries value: HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount]

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

Queries value:

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f(fdd39ad0-238f-46af-adb4-6c85480369c7)\cite{Control of the control of the c$

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\soft\windows\currentversion\explorer\folderdescriptions\fdd39ad0-238f-46af-adb4-6c85480369c7\\ [relative path]$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\\folderdescriptions\\fdd39ad0-238f-46af-adb4-6c85480369c7\\[infotip]$

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-bound} $HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fdd39ad0-238f-46af-adb4-6c85480369c7\[security]$

Queries value:

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

Queries value:

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\f(fdd39ad0-238f-46af-adb4-6c85480369c7)\[streamresourcetype]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\\folderdescriptions\\fdd39ad0-238f-46af-adb4-6c85480369c7\\[localredirectonly]$

Queries value:

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

Oueries value:

Oueries value:

 $\label{lem:hklmsoftwarewow6432} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \fdd 39 ad 0-238f-46af-ad b4-6c85480 369 c7 \fter \figure{1.5cm} \full \figure{1.5cm} \figure{1.5cm}$

Oueries value:

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

Queries value:

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

Queries value:

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

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

f20f-4863-afef-f87ef2e6ba25}[localredirectonly]

Queries value:

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

Queries value:

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

Oueries value:

Oueries value:

Oueries value:

Queries value:

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

Queries value:

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

Queries value: $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\user shell folders[common desktop]

Queries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer[turn off spianimations]$

Sets/Creates value:

HKCU\software\headlight\getrighttogo\customizedapps[c1a5167faf749c474083cf838ee771c6]

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]