Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3311, Task ID: 753

Task ID: 753 Risk Level: 10

Date Processed: 2016-05-18 10:34:08 (UTC)

Processing Time: 62.08 seconds
Virtual Environment: IntelliVM

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

Sample ID: 3311
Type: basic
Owner: admin

Label: 2a29e3a5d469fbc803a504464393f98e

Date Added: 2016-05-18 10:30:49 (UTC)

File Type: PE32:win32:gui File Size: PE32:win32:gui

MD5: 2a29e3a5d469fbc803a504464393f98e

SHA256: c16b99b6dd2073d18c21dc2a0a24ba4b99355ab89405e9abf1d902d7f841f5cd

Description: None

Pattern Matching Results

10 Creates malicious mutex: DarkComet [APT, RAT]

7 Writes to memory of system processes

7 YARA score 7

5 Possible injector

4 Connects to local IP

7 Injects thread into Windows process

Static Events

YARA rule hit: KeyLoggerStrings

Anomaly: PE: Contains a virtual section

Process/Thread Events

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

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

Creates process: C:\Windows\system32\notepad.exe [notepad]
Writes to process: PID:2268 C:\Windows\System32\notepad.exe

Creates remote thread: C:\Windows\System32\notepad.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex: \Sessions\1\BaseNamedObjects\DC_MUTEX-F5BOMXB
Creates mutex: \Sessions\1\BaseNamedObjects\DCPERSFWBP
Creates event: \KernelObjects\MaximumCommitCondition

File System Events

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

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

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

Opens: C:\Windows\System32

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

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

controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af

Opens: C:\windows\temp\winmm.dll Opens: C:\Windows\System32\winmm.dll Opens: C:\windows\temp\netapi32.dll Opens: C:\Windows\System32\netapi32.dll Opens: C:\windows\temp\netutils.dll Opens: C:\Windows\System32\netutils.dll Opens: C:\windows\temp\srvcli.dll Opens: C:\Windows\System32\srvcli.dll C:\windows\temp\wkscli.dll Opens: C:\Windows\System32\wkscli.dll Opens:

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

Opens: C:\windows\temp\msacm32.dll
Opens: C:\Windows\System32\msacm32.dll

```
C:\windows\temp\SHFolder.dll
 Opens:
 Opens:
                         C:\Windows\System32\shfolder.dll
 Opens:
                         C:\windows\temp\AVICAP32.DLL
 Opens:
                         C:\Windows\System32\avicap32.dll
 Opens:
                         C:\windows\temp\MSVFW32.dll
 Opens:
                         C:\Windows\System32\msvfw32.dll
 Opens:
                         C:\Windows\System32\imm32.dll
                         C:\Windows\System32\en-US\msvfw32.dll.mui
 Opens:
 Opens:
                         C:\Windows\System32\en-US\avicap32.dll.mui
 Opens:
                         C:\windows\temp\2a29e3a5d469fbc803a504464393f98e.ENU
 Opens:
                         C:\windows\temp\2a29e3a5d469fbc803a504464393f98e.ENU.DLL
 Opens:
                         C:\windows\temp\2a29e3a5d469fbc803a504464393f98e.EN
 Opens:
                         C:\windows\temp\2a29e3a5d469fbc803a504464393f98e.EN.DLL
 Opens:
                         C:\Windows\System32\uxtheme.dll
 Opens:
                         C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens:
                         C:\windows\temp\dwmapi.dll
 Opens:
                         C:\Windows\System32\dwmapi.dll
 Opens:
                         C:\Windows\Fonts\StaticCache.dat
 Opens:
                         C:\Windows\System32\en-US\user32.dll.mui
 Opens:
                         C:\Windows\System32\rpcss.dll
 Opens:
                         C:\windows\temp\CRYPTBASE.dll
 Opens:
                         C:\Windows\System32\cryptbase.dll
 Opens:
                         C:\windows\temp\PSymSE8rHgHi.dcp
 Opens:
                         C:\
 Opens:
                         C:\Windows\system32\PSymSE8rHgHi\
 Opens:
                         C:\Program Files
 Opens:
                         C:\Windows\system32\notepad
                         C:\Windows\Temp\2a29e3a5d469fbc803a504464393f98e.exe
 Opens:
 Opens:
                         C:\windows\temp\notepad.exe
 Opens:
                         C:\Windows\System32\notepad.exe
 Opens:
                         C:\Windows\System32\apphelp.dll
 Opens:
                         C:\Windows\Prefetch\NOTEPAD.EXE-D8414F97.pf
 Opens:
                         C:\Users\Admin\AppData\Roaming
 Opens:
                         C:\Windows\System32\shell32.dll
                         C:\Windows\winsxs\x86_microsoft.windows.common-
 Opens:
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
                         C:\Windows\WindowsShell.Manifest
 Opens:
 Opens:
                         C:\Windows\system32\notepad.exe.Local\
                         C:\Windows\System32\winspool.drv
 Opens:
 Opens:
                         C:\Windows\System32\propsys.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
                         C:\windows\temp\ntmarta.dll
 Opens:
 Opens:
                         C:\Windows\System32\ntmarta.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000006.db
 Opens:
                         C:\Users\desktop.ini
 Opens:
                         C:\Windows\System32\en-US\setupapi.dll.mui
                         C:\Users
 Opens:
 Opens:
                         C:\Users\Admin
 Opens:
                         C:\Users\Admin\AppData
                         C:\Users\Admin\Desktop\desktop.ini
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Roaming\dclogs\
 Opens:
                         C:\Users\Admin\AppData\Roaming\dclogs
 Opens:
 Opens:
                         C:\Windows
 Opens:
                         C:\Windows\Fonts
 Opens:
                         C:\Windows\System32\mswsock.dll
 Opens:
                         C:\Windows\System32\WSHTCPIP.DLL
 Opens:
                         C:\Windows\System32\en-US\notepad.exe.mui
 Opens:
                         C:\Windows\Globalization
 Opens:
                         C:\Windows\Globalization\Sorting
 Opens:
                         C:\Windows\ServiceProfiles
                         C:\Windows\ServiceProfiles\NetworkService
 Opens:
 Opens:
                         C:\Windows\ServiceProfiles\NetworkService\AppData
 Opens:
                         C:\Windows\ServiceProfiles\NetworkService\AppData\Local
                         {\tt C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft}
 Opens:
 Opens:
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player NSS
 Opens:
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player NSS\3.0
 Opens:
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player
NSS\3.0\Icon Files
 Opens:
                         C:\Windows\Svstem32\en-US
                         C: \verb|\windows\System32\ntdll.dll|\\
 Opens:
 Opens:
                         C:\Windows\System32\kernel32.dll
 Opens:
                         C:\Windows\System32\apisetschema.dll
 Opens:
                         C:\Windows\System32\KernelBase.dll
 Opens:
                         C:\Windows\System32\locale.nls
 Opens:
                         C:\Windows\System32\advapi32.dll
 Opens:
                         C:\Windows\System32\msvcrt.dll
```

C:\Windows\System32\rpcrt4.dll Opens: Opens: C:\Windows\System32\gdi32.dll C:\Windows\System32\user32.dll Opens: Opens: C:\Windows\System32\lpk.dll Opens: C:\Windows\System32\usp10.dll Opens: C:\Windows\System32\comdlg32.dll Opens: C:\Windows\System32\shlwapi.dll C:\Windows\System32\ole32.dll Opens: C:\Windows\System32\oleaut32.dll Opens: Opens: C:\Windows\System32\msctf.dll Opens: C:\Windows\System32\imageres.dll

C:\Windows\System32\en-US\imageres.dll.mui Opens:

Opens:

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player

NSS\3.0\Icon Files\0aef9a97-98cd-4f89-b183-3db737149306.png C:\Windows\System32\slui.exe C:\Windows\System32\sppsvc.exe Opens: Opens: C:\Windows\system32\uxtheme.dll.Config Opens: C:\Windows\Fonts\lucon.ttf

Reads from: C:\Windows\Fonts\StaticCache.dat C:\Windows\Prefetch\NOTEPAD.EXE-D8414F97.pf Reads from:

Reads from: C:\Users\desktop.ini

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

Network Events

Connects to: 192.168.0.149:100

Windows Registry Events

Creates key: HKCU\software Creates key: HKCU\software\dc3_fexec Opens key: HKLM\system\currentcontrolset\control\session manager 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\policies\microsoft\windows\safer\codeidentifiers Opens key: $\label{lem:hkcu} \mbox{HKCU\software\policies\mbox{\verb|microsoft\windows\safer\codeidentifiers}$}$ Opens key: HKCU\ HKCU\control panel\desktop\muicached\machinelanguageconfiguration Opens key: HKLM\software\policies\microsoft\mui\settings Opens key: Opens key: HKCU\software\policies\microsoft\control panel\desktop HKCU\control panel\desktop\languageconfiguration Opens key: Opens key: HKCU\control panel\desktop Opens key: HKCU\control panel\desktop\muicached HKLM\software\microsoft\windows\currentversion\sidebyside Opens kev: Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots HKLM\system\currentcontrolset\control\nls\sorting\versions Opens key: Opens key: HKLM\system\currentcontrolset\control\error message instrument\ Opens key: HKLM\system\currentcontrolset\control\error message instrument Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize Opens key: $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus compatibility 32$ Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility Opens key: HKLM\ Opens key: $\label{lem:hklm} \mbox{HKLM} \mbox{$\mbox{hklm}\software\mbox{$\mbox{microsoft}\windows}$} \mbox{$\mbox{nt}\currentversion} \mbox{$\mbox{windows}$} \mbox{$\mbox{hklm}\software} \mbox{$\mbox{hklm}\software} \mbox{$\mbox{hklm}\software} \mbox{$\mbox{hklm}\software} \mbox{$\mbox{hklm}\software} \mbox{$\mbox{hklm}\software} \mbox{$\mbox{hklm}\software} \mbox{$\mbox{hklm}\software} \mbox{$\mbox{hklm}\software} \mbox{\mbox{hklm}\software} \mbox{\mbox{hklm}\software} \mbox{\mbox{\mbox{hklm}\software} \mbox{\mbox{\mbox{hklm}\software}} \mbox{\mbox{\mbox{\mbox{hklm}\software}} \mbox{\mbox$ HKLM\software\microsoft\ole Opens key: Opens key: HKLM\software\microsoft\ole\tracing Opens key: HKLM\software\microsoft\oleaut Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics HKLM\system\currentcontrolset\services\crypt32 Opens key: Opens key: HKLM\software\microsoft\windows\currentversion\internet settings Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings Opens key: $\label{lem:hklm} \verb+Kklm \system \current control set \services \verb+ lanman work station \parameters \\$ HKLM\system\currentcontrolset\control\cmf\config Opens key: HKLM\software\microsoft\windows\windows error reporting\wmr Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\vfw Opens key: HKCU\software\borland\locales HKLM\software\borland\locales Opens kev: Opens key: HKCU\software\borland\delphi\locales Opens key: HKLM\system\currentcontrolset\control\nls\customlocale Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes Opens key: HKLM\system\currentcontrolset\control\nls\locale Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts Opens key: HKLM\system\currentcontrolset\control\nls\language groups Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink HKLM\software\microsoft\windows Opens key:

nt\currentversion\languagepack\surrogatefallback HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\segoe ui

HKLM\software\microsoft\windows

nt\currentversion\languagepack\datastore_v1.0

Opens key:

Opens key: HKLM\hardware\devicemap\video

HKLM\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-Opens kev:

fd27e3774e32}\0000

Opens key:

HKLM\system\currentcontrolset\enum\pci\ven_80ee&dev_beef&subsys_00000000&rev_00\3&267a616a&0&10

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

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

Opens key: HKLM\svstem\currentcontrolset\services\winsock2\parameters

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog

Opens key:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus appid_catalog \setminus 0.86496d7$

Opens key:

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019 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:

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007 Opens key:

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010 Opens key:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ (catalog_entries \ 0000000000011) \ (catalog_entries \ (catalog \ (catalog_entries \ (catalog \ (cata$ Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000013 Opens key:

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

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog9 \ (catalog_entries) \ 000000000015$ Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000016 Opens key:

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

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

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

Opens key:

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003 Opens kev:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000005 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006

Opens kev: HKLM\software\microsoft\rpc

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

Opens key: HKLM\system\setup

Opens key: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKLM\svstem\currentcontrolset\control\idconfigdb

Opens key: HKLM\system\currentcontrolset\control\idconfigdb\hardware profiles\0001

Opens kev: HKLM\system\currentcontrolset\control\idconfigdb\currentdockinfo

Opens key:

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

Opens key:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-

b29c-65b732d3d21a}

Opens key:

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

b29c-65b732d3d21a}\propertybag

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

Opens kev:

HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings

Opens key: HKCU\software\dc3_fexec
Opens key: HKCU\software\dc2 users

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

options\notepad.exe

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

Opens key: HKLM\software\policies\microsoft\windows\appcompat
Opens key: HKCU\software\microsoft\windows nt\currentversion

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

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

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

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

options Opens key:

a03a-e3ef65729f3d}

Opens key:

a03a-e3ef65729f3d}\propertybag

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

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

Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders

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

folders

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

Opens key:

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

Opens key: HKCU\software\classes\

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

08002b30309d}\shellfolder

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

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

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

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

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

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

Opens key:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \mbox{microsoft \windows \current version \explorer \mbox{mountpoints 2$ \cpc \volume} \end{tabular} \label{lem:hkcu}$

Opens key:

11e3-b3bc-806e6f6e6963}\

Opens key: ${\tt HKCU \setminus software \setminus classes \setminus drive \setminus shellex \setminus folder extensions}$

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

Opens key: HKLM\software\microsoft\com3

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

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

b8dc300d9f9d}\treatas

Opens key: $\label{eq:hkcr} \begin{tabular}{ll} HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas \\ Opens key: \\ HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-b8dc30d9f9d}\treatas \\ \begin{tabular}{ll} HKCU\software\classes\clsid\fractarrange\c$

b8dc300d9f9d}\progid

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

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

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

b8dc300d9f9d}\inprochandler32

Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d\inprochandler

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

Opens key: ${\tt HKLM \ } {\tt KLM \ } {\tt LKLM \ } {\tt LKL$

Opens key: HKLM\system\currentcontrolset\services\ldap
Opens key: HKLM\software\microsoft\windows\currentversion

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

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

Opens key:

 $HKLM \ software \ microsoft \ windows \ shell \ registered applications \ urlass ociations \ directory \ open with progids$

Opens key:

 $\label{thm:local_hammon} \begin{tabular}{l} HKCU \software \verb|microsoft| windows \shell \associations \urlassociations \associations \associa$

HKCU\software\classes\directory Opens key:

Opens key: HKCR\directorv

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

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

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

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

Opens key: HKCR\folder

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

HKCR\folder\shellex\iconhandler Opens key:

Opens key: HKCU\software\classes\allfilesystemobjects

Opens key: HKCR\allfilesystemobjects

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

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

Opens key: HKCR\directory\docobject

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

Opens key: HKCR\folder\docobject

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

Opens key: HKCR\allfilesystemobjects\docobject

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

HKCR\directory\browseinplace Opens key:

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

Opens key: HKCR\folder\browseinplace

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

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

HKCR\directory\clsid Opens key:

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:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}

Opens key:

 $HKLM \ software \ microsoft \ windows \ current version \ (b4bfcc3a-db2c-424c-db2c-42b) \ descriptions \ (b4bfcc3a-db2c-424c-db2c-42b) \ descriptions \ de$ b029-7fe99a87c641}\propertybag

Opens kev:

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

Opens key:

 $HKLM \ software \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b2$

b4ef-bd1dc332aeae}\propertybag

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

Opens key:

11e3-b3bc-806e6f6e6963}\

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

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

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

migration\providers\psched

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

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

migration\providers\tcpip

Opens key: HKCU\software\microsoft\notepad

Opens key: ${\it HKLM \ } software \verb|\ microsoft \ | notepad \verb|\ default fonts |$ Queries value: HKLM\system\currentcontrolset\control\session

manager[cwdillegalindllsearch]

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

Oueries value:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [transparentenabled]$

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

 $\label{lem:hkcu} \verb|HKCU| control panel| desktop| \verb|muicached[machinepreferreduil] anguages]| \\$ Queries value:

Oueries value:

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

nt\currentversion\compatibility32[2a29e3a5d469fbc803a504464393f98e]

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\windows[loadappinit_dlls]

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

```
Queries value:
                                     HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
                                     \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
  Oueries value:
settings[disableimprovedzonecheck]
  Queries value:
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
  Queries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]
                                     HKLM\system\currentcontrolset\control\cmf\config[system]
  Oueries value:
  Queries value:
                                     HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Oueries value:
                                     HKLM\svstem\currentcontrolset\control\nls\extendedlocale[en-us]
  Queries value:
                                     \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + nt + current version + fontsubstitutes [ms]
shell dlg 2]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\language groups[1]
  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]|
                                     HKLM\software\microsoft\windows
  Queries value:
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\hardware\devicemap\video[maxobjectnumber]
  Oueries value:
  Queries value:
                                     HKLM\hardware\devicemap\video[\device\video3]
  Queries value:
                                     HKLM \ system \ current control \ video \ \{c54b6caf-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab56-be91-4a10-ab
fd27e3774e32}\0000[pruningmode1
  Queries value:
                                     HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
  Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9[next catalog entry id]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 000000000001 \ [packed catalog item]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  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\000000000004[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000005[packedcatalogitem]
  Queries value:
```

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ 0000000000007 \ [packed catalog item]$

Oueries value:

Queries value:

Queries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 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\00000000001[displaystring]
 Queries 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\000000000001[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\00000000001[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
- 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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[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\00000000003[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
 Queries 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[displaystring]
 Oueries value:

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\000000000004[supportednamespace] Oueries value:

Oueries value:

Oueries value:

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

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog 5 \setminus catalog_entries \setminus 0000000000004 [provider info]$ Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace _catalog5 \ catalog_entries \ 000000000005 [library path]$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring] Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap amespace_catalog \\ S \setminus catalog_entries \setminus 0000000000005[providerid]$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily] Queries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ (catalog_entries \ 0000000000005 [supported namespace]]$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled] Queries value:

Queries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace_catalog_entries \ (000000000005[storesserviceclass info]) \ (catalog_entries) \$ Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog 5 \setminus catalog_entries \setminus 0000000000005[provider info]$ Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace _catalog5 \ catalog_entries \ 000000000006 [library path]$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000006[displaystring] Oueries value:

Oueries 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\00000000006[enabled] Oueries value:

Oueries value:

 $HKLM \ system \ (current control set \ services \ win sock 2 \ parameters \ names pace_catalog_entries \ (00000000006[storesserviceclass info]) \ (control set \ names \ nam$ Queries value:

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2 32spincount1 Queries value: HKLM\software\microsoft\rpc[maxrpcsize]

Queries value:

HKLM\system\currentcontrolset\control\computername\activecomputername[computername]

Queries value: HKLM\system\setup[oobeinprogress] Queries value: HKLM\system\setup[systemsetupinprogress]

Oueries value: HKLM\system\currentcontrolset\control\idconfigdb[currentconfig]

Oueries value: Queries value:

HKLM\system\currentcontrolset\control\idconfigdb\currentdockinfo[dockingstate]

HKLM\system\currentcontrolset\control\idconfigdb\hardware

profiles\0001[hwprofileguid]

Queries value:

profiles\0001[friendlyname]

Oueries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ 'folder descriptions \ '\{905e63b6-c1bf-494e-descriptions \ 'explorer' \ 'explorer'' \ 'explorer' \ 'explorer' \ 'explorer' \ 'explorer'' \ 'explor$

b29c-65b732d3d21a}[category]

Oueries value:

 $HKLM \ software \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \ \{905e63b6-c1bf-494e-d1$ b29c-65b732d3d21a}[name]

Oueries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ 'folder descriptions \ '\{905e63b6-c1bf-494e-descriptions \ 'explorer' \ 'explorer'' \ 'explorer' \ 'explorer' \ 'explorer' \ 'explorer'' \ 'explor$ b29c-65b732d3d21a}[parentfolder]

Queries value:

 $HKLM \ software \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \ \{905e63b6-c1bf-494e-d1$ b29c-65b732d3d21a}[description]

Queries value:

b29c-65b732d3d21a}[relativepath]

Oueries value:

 $HKLM \ software \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \ \{905e63b6-c1bf-494e-d1$

b29c-65b732d3d21a}[parsingname]

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a\}[infotip]} Infotip \cite{Continuous of the continuous of the continuo$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{905e63b6-c1bf-494e-b29c-65b732d3d21a\}[localized name]$

Queries value:

 $HKLM \ software \ `microsoft \ 'entre \ 'entre$

Queries value:

 $HKLM \ software \ `microsoft \ 'entre \ 'entre$

Queries value:

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

Queries value:

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

Queries value

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} \ [publish \ expanded path]$

Queries value

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

Oueries value

 $\label{local-prop} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\gamma\$

Queries value:

 $\label{lem:hkk} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a\}[initfolderhandler]}$

Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir]

Oueries value:

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options[disablelocaloverride]

Queries value: HKCU\software\dc3_fexec[{e29ac6c0-7037-11de-816d-806e6f6e6963-

1087083969}]

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\sinous \current version \explorer\folder descriptions \current \curre$

Queries value:

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

Queries value:

 $\label{local-HKLM-software-microsoft-windows-current-version-explorer-folder-descriptions-fabs-65f9-4cf6-a03a-e3ef65729f3d} [parentfolder]$

Oueries value:

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

Queries value:

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

Oueries value:

 $\label{lem:hklm} HKLM software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hklm} a 03a-e 3e f 65 72 9f 3d \cal{lem:hklm} [par sing name]$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \called \footnote{1.00} \called \footnot$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \mbox{$microsoft\windows\currentversion} explorer \folder descriptions \folds folder descriptions \folds folds folder descriptions \folds folds folds folder descriptions \folds folds folds$

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} current version \explorer \folder descriptions \folder \folder descriptions \folder descriptions \folder \folder$

Queries value:

```
a03a-e3ef65729f3d}[streamresourcetype]
 Oueries value:
a03a-e3ef65729f3d}[localredirectonly]
 Oueries value:
a03a-e3ef65729f3d}[roamable]
 Oueries value:
a03a-e3ef65729f3d}[precreate]
 Oueries value:
a03a-e3ef65729f3d}[stream]
 Oueries value:
a03a-e3ef65729f3d}[publishexpandedpath]
 Oueries value:
a03a-e3ef65729f3d}[attributes]
 Queries value:
a03a-e3ef65729f3d}[foldertypeid]
 Oueries value:
a03a-e3ef65729f3d}[initfolderhandler]
                   \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ explorer \verb+ user shell
 Queries value:
folders[appdata]
 Queries value:
                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries value:
08002b30309d}\shellfolder[callforattributes]
                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries value:
08002b30309d}\shellfolder[restrictedattributes]
 Queries value:
                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsfordisplay]
                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries value:
08002b30309d}\shellfolder[hidefolderverbs]
 Oueries value:
                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[usedrophandler]
                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries value:
08002b30309d}\shellfolder[wantsforparsing]
                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
 Queries value:
                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforoverlay]
                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries value:
08002b30309d}\shellfolder[mapnetdriveverbs]
 Queries value:
                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforinfotip]
 Queries value:
                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideinwebview]
                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
 Oueries value:
08002b30309d}\shellfolder[hideondesktopperuser]
                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
 Queries value:
                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsuniversaldelegate]
                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
 Oueries value:
08002b30309d}\shellfolder[nofilefolderjunction]
                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries value:
08002b30309d}\shellfolder[pintonamespacetree]
 Queries value:
                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hasnavigationenum]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}1
 Queries value:
11e3-b3bc-806e6f6e6963}[data]
 Oueries value:
11e3-b3bc-806e6f6e6963}[generation]
                   HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
 Oueries value:
409d6c4515e9}[drivemask]
 Queries value:
                   HKLM\software\microsoft\com3[com+enabled]
 Oueries value:
                   HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
 Queries value:
                   HKCR\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[inprocserver32]
                   HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[]
 Oueries value:
 Oueries value:
                   HKCR\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[threadingmodel]
```

HKLM\software\microsoft\ole[maxsxshashcount]

Queries value: Queries value: HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension] Oueries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity] Oueries value: HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder] HKLM\system\currentcontrolset\services\ldap[usehostnameasalias] Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath] Oueries value: Queries value: HKLM\software\microsoft\windows\currentversion[devicepath] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview] HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter] Oueries value: Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden] Queries value: $HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced \ [separate process]$ Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly] Queries value: $HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced [show type overlay]$ HKCR\directory[docobject] Queries value: HKCR\folder[docobject] Oueries value: Oueries value: HKCR\allfilesystemobjects[docobject] HKCR\directory[browseinplace] Queries value: HKCR\folder[browseinplace] Queries value: Oueries value: HKCR\allfilesystemobjects[browseinplace] HKCR\directory[isshortcut] Queries value: HKCR\folder[isshortcut] Oueries value: Queries value: HKCR\allfilesystemobjects[isshortcut] HKCR\directory[alwaysshowext] Oueries value: Queries value: HKCR\directory[nevershowext] Queries value: HKCR\folder[nevershowext] Queries value: HKCR\allfilesystemobjects[nevershowext] Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[category] Oueries value: b029-7fe99a87c641}[name] Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[parentfolder] Oueries value: b029-7fe99a87c641}[description] Queries value: b029-7fe99a87c641}[relativepath] Oueries value: b029-7fe99a87c641}[parsingname] Queries value: b029-7fe99a87c641}[infotip] Oueries value: b029-7fe99a87c641}[localizedname] Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[icon] Oueries value: b029-7fe99a87c641}[security] Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-

b029-7fe99a87c641}[streamresource]

Oueries value:

b029-7fe99a87c641}[streamresourcetype]

Queries value:

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

Oueries value:

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

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ (b4bfcc3a-db2c-424c-b029-7fe99a87c641) \ [precreate]$

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

folders[desktop]

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ 'entre \ 'folder descriptions \ '\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [roamable]$

Queries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ 's ream' \ explorer \ 'folder descriptions \ '\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [stream]$

Queries value:

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

Queries value:

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

Queries value:

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

b4ef-bd1dc332aeae}[foldertypeid]

Queries value:

b4ef-bd1dc332aeae}[initfolderhandler]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\compatibility32[notepad]

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

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

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

Queries value:

 $\label{local-basis} HKCU software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ \{69d250e3-6c18-11e3-b3bc-806e6f6e6963\} \ [data]$

Oueries value:

 $\label{lem:hkcu} HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{69d250e3-6c18-11e3-b3bc-806e6f6e6963\}[generation]}$

 $\label{thm:parameters} Queries \ value: \\ HKLM \ system \ current controls et \ services \ winsock \ parameters [transports]$

Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]

Queries value:

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

migration\providers\psched[winsock 2.0 provider id]

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

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

migration\providers\tcpip[winsock 2.0 provider id]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]

Queries value:

Queries value:

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]

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

 Queries value:
 HKCU\software\microsoft\notepad[1fpitchandfamily]

 Queries value:
 HKLM\software\microsoft\notepad\defaultfonts[1ffacename]

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

Queries value: HKCU\software\microsoft\notepad[1ffacename]
Queries value: HKCU\software\microsoft\notepad[ipointsize]
Queries value: HKCU\software\microsoft\notepad[fwrap]
Queries value: HKCU\software\microsoft\notepad[statusbar]

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

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