# Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 129, Task ID: 516

Task ID: 516 Risk Level: 6

Date Processed: 2016-04-28 13:01:20 (UTC)

Processing Time: 3.08 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\adb62392bc0711707e58e70186cc4ac2.exe"

Sample ID: 129
Type: basic
Owner: admin

Label: adb62392bc0711707e58e70186cc4ac2

Date Added: 2016-04-28 12:45:03 (UTC)

File Type: PE32:win32:gui File Size: 10224 bytes

MD5: adb62392bc0711707e58e70186cc4ac2

SHA256: 2d34179da23d345fb5e9d241b34902c188fbf914f3985a7ffb3978dd9ff0287b

Description: None

### Pattern Matching Results

4 Terminates process under Windows subfolder

6 Renames file on boot

#### Process/Thread Events

Creates process: C:\windows\temp\adb62392bc0711707e58e70186cc4ac2.exe

["C:\windows\temp\adb62392bc0711707e58e70186cc4ac2.exe" ]

Creates process: C:\Windows\system32\schtasks.exe ["C:\Windows\system32\schtasks.exe"

/Delete /TN EPUpdater /F]

Terminates process: C:\Windows\Temp\adb62392bc0711707e58e70186cc4ac2.exe

Terminates process: C:\Windows\System32\schtasks.exe

#### Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

 $\label{lem:creates} Creates \ mutex: $$ \Sessions\1\BaseNamedObjects\ZonesCounterMutex $$$ 

Creates mutex: \Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex

Creates mutex: \Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex
Creates mutex: \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex

Creates event: \KernelObjects\MaximumCommitCondition

Creates event: \Security\LSA\_AUTHENTICATION\_INITIALIZED
Creates event: \BaseNamedObjects\ConsoleEvent-0x00000988
Creates event: \BaseNamedObjects\SvcctrlStartEvent\_A3752DX

## File System Events

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

Opens: C:\Windows\Prefetch\ADB62392BC0711707E58E70186CC4-219A86D2.pf

Opens: C:\Windows\System32

Opens: C:\Windows\System32\sechost.dll
Opens: C:\Windows\System32\imm32.dll

Opens: C:\Windows\Globalization\Sorting\SortDefault.nls

Opens: C:\Users\Admin\AppData\Roaming

Opens: C:\Users\Admin\AppData\Roaming\BabSolution\Shared\BUSolution.dll

Opens: C:\Windows\System32\rpcss.dll C:\windows\temp\CRYPTBASE.dll Opens: Opens: C:\Windows\System32\cryptbase.dll Opens: C:\Windows\System32\uxtheme.dll Opens: C:\Windows\System32\schtasks.exe Opens: C:\windows\temp\PROPSYS.dll Opens: C:\Windows\System32\propsys.dll Opens: C:\Windows\System32\shell32.dll

Opens: C:\windows\temp\adb62392bc0711707e58e70186cc4ac2.exe.Local\

Opens: C:\Windows\winsxs\x86\_microsoft.windows.common-

controls\_6595b64144ccf1df\_6.0.7601.17514\_none\_41e6975e2bd6f2b2

Opens: C:\Windows\winsxs\x86\_microsoft.windows.common-controls\_6595b64144ccf1df\_6.0.7601.17514\_none\_41e6975e2bd6f2b2\comctl32.dll

Opens: C:\Windows\WindowsShell.Manifest

Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db

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

Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-

4C77-AF34-C647E37CA0D9}.1.ver0x000000000000006.db

Opens: C:\Users\Admin\Desktop\desktop.ini

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

Opens: C:\Windows\System32\urlmon.dll
Opens: C:\windows\temp\SspiCli.dll
Opens: C:\Windows\System32\sspicli.dll

Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files

Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies

Opens: C:\

Opens: C:\Windows

Opens: C:\Windows\system32\schtasks.exe:Zone.Identifier
Opens: C:\Windows\System32\en-US\setupapi.dll.mui

Opens: C:\Windows\System32\apphelp.dll

Opens: C:\Windows\Temp\adb62392bc0711707e58e70186cc4ac2.exe

Opens: C:\Windows\Prefetch\SCHTASKS.EXE-5CA45734.pf

Opens: C:\Windows\System32\ktmw32.dll

Opens: C:\Windows\System32\en-US\schtasks.exe.mui

Opens: C:\Windows\System32\version.dll
Opens: C:\Windows\System32\taskschd.dll

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

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

## Windows Registry Events

Creates key: HKLM\system\currentcontrolset\control\session manager
Deletes value: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap[proxybypass]

Deletes value: HKLM\software\microsoft\windows\currentversion\internet

settings\zonemap[proxybypass]

Deletes value: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap[intranetname]

Deletes value: HKLM\software\microsoft\windows\currentversion\internet

settings\zonemap[intranetname]

Opens key: HKLM\system\currentcontrolset\control\session manager
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: HKCU\software\policies\microsoft\windows\safer\codeidentifiers

Opens key: HKCU\

Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration

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

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\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
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\software\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility

Opens key: HKLM\

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

Opens key:

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

Opens key: HKLM\software\microsoft\ole

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

Opens key:

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

Opens key:

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

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

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

Opens key:

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

folders

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

Opens key:

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

Opens key:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1ac14e77-02e7-4e5d-14e74-1$ 

b744-2eb1ae5198b7}

Opens key:

 $HKLM \setminus software \setminus irrestant + windows \setminus current + version \setminus explorer \setminus folder descriptions \setminus \{1ac14e77-02e7-4e5d-14e74$ 

b744-2eb1ae5198b7}\propertybag

Opens kev:

HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\adb62392bc0711707e58e70186cc4ac2.exe

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

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

Opens key: HKLM\software\microsoft\oleaut

Opens key:

HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
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: HKCU\software\classes\drive\shellex\folderextensions

Opens key: HKCR\drive\shellex\folderextensions

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

4442-804e-409d6c4515e9}

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

409d6c4515e9}

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

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

Opens key: HKCU\software\classes\.exe

Opens key: HKCR\.exe

Opens key: HKCU\software\classes\.exe\openwithprogids

Opens key: HKCR\.exe\openwithprogids

Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.exe\openwithprogids

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

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.exe

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.exe\

Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.exe\userchoice

Opens key: HKCU\software\classes\exefile

Opens key: HKCR\exefile

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

Opens key: HKCR\exefile\curver

Opens key: HKCR\exefile\

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

Opens key: HKCR\exefile\shellex\iconhandler

Opens key: HKCU\software\classes\systemfileassociations\.exe

Opens key: HKCR\systemfileassociations\.exe

Opens key: HKCU\software\classes\systemfileassociations\.exe\shellex\iconhandler

Opens key: HKCR\systemfileassociations\.exe\shellex\iconhandler

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

Opens key: HKCR\exefile\docobject

Opens key: HKCU\software\classes\systemfileassociations\.exe\docobject

Opens key: HKCR\systemfileassociations\.exe\docobject
Opens key: HKCU\software\classes\exefile\browseinplace

Opens key: HKCR\exefile\browseinplace

Opens key: HKCU\software\classes\systemfileassociations\.exe\browseinplace

Opens key: HKCR\systemfileassociations\.exe\browseinplace

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

Opens key: HKCR\exefile\clsid

Opens key: HKCU\software\classes\systemfileassociations\.exe\clsid

Opens key: HKCR\systemfileassociations\.exe\clsid

Opens key:

b029-7fe99a87c641}

Opens key:

b029-7fe99a87c641}\propertybag

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

b8dc300d9f9d}\inprocserver32

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

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

b8dc300d9f9d}\inprochandler32

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

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

Opens key:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1b3ea5dc-b587-4786-b364, and \ b36ab4, and \ b$ 

b4ef-bd1dc332aeae}

Opens key:

 $\label{thm:local_thm} \begin{tabular}{ll} HKLM\software\mbox{\scale=converted} & \label{thm:local_thm} \end{tabular} $$HKLM\software\mbox{\scale=converted} & \label{thm:local_thm} $$HKLM\software\mbox{\scale=converted} & \label{thm:local_thm:lo$ 

b4ef-bd1dc332aeae}\propertybag

Opens key:

9afe-ea3317b67173}

Opens key:

9afe-ea3317b67173}\propertybag

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

2160590473-689474908-1361669368-1002

Opens key:

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

Opens key:

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

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

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

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

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

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

Opens key: HKCR\folder

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

Opens key: HKCR\folder\shellex\iconhandler

Opens key: HKCU\software\classes\allfilesystemobjects

Opens key: HKCR\allfilesystemobjects

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

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

Opens key: HKCR\directory\docobject

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

Opens key: HKCR\folder\docobject

Opens key:  ${\tt HKCU \setminus software \setminus classes \setminus all filesystemobjects \setminus docobject}$ 

Opens key: HKCR\allfilesystemobjects\docobject

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

Opens key: HKCR\directory\browseinplace

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

Opens key: HKCR\folder\browseinplace

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

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

Opens key: HKCR\directory\clsid

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

Opens key: HKCR\folder\clsid

Opens key:  ${\sf HKCU \backslash software \backslash classes \backslash allfilesystemobjects \backslash clsid}$ 

```
HKCR\allfilesystemobjects\clsid
  Opens key:
  Opens key:
                                        HKLM\software\microsoft\windows\currentversion\explorer\kindmap
  Opens key:
                                        HKLM\system\currentcontrolset\control\cmf\config
  Opens key:
                                        HKLM\software\microsoft\windows\windows error reporting\wmr
  Opens key:
                                        HKCU\software\classes\exefile\shell
  Opens key:
                                        HKCR\exefile\shell
  Opens key:
                                        HKCU\software\classes\exefile\shell\open
  Opens key:
                                        HKCR\exefile\shell\open
  Opens key:
                                        HKCR\exefile\shell\open\
                                        HKCU\software\classes\exefile\shell\open\command
  Opens key:
  Opens key:
                                        HKCR\exefile\shell\open\command
  Opens key:
                                        HKCU\software\classes\exefile\shell\open\droptarget
  Opens key:
                                        HKCR\exefile\shell\open\droptarget
                                        HKLM\software\microsoft\windows\currentversion\policies\associations
  Opens key:
  Opens key:
                                        HKCU\software\microsoft\windows\currentversion\policies\associations
  Opens key:
                                        HKCU\software\classes\.ade
  Opens key:
                                        HKCR\.ade
  Opens key:
                                        HKCU\software\classes\.adp
  Opens key:
                                        HKCR\.adp
  Opens key:
                                        HKCU\software\classes\.app
  Opens key:
                                        HKCR\.app
  Opens key:
                                        HKCU\software\classes\.asp
  Opens key:
                                        HKCR\.asp
  Opens key:
                                        HKCU\software\classes\.bas
  Opens key:
                                        HKCR\.bas
                                        HKCU\software\classes\.bat
  Opens key:
  Opens key:
                                        HKCR\.bat
  Opens key:
                                        HKCU\software\classes\.cer
  Opens key:
                                        HKCR\.cer
  Opens key:
                                        HKCU\software\classes\.chm
  Opens key:
                                        HKCR\.chm
  Opens key:
                                        HKCU\software\classes\.cmd
  Opens key:
                                        HKCR\.cmd
  Opens key:
                                        HKCU\software\classes\.com
  Opens key:
                                        HKCR\.com
  Opens key:
                                        HKCU\software\classes\.cpl
  Opens key:
                                        HKCR\.cpl
  Opens key:
                                        HKCU\software\classes\.crt
                                        HKCR\.crt
  Opens key:
  Opens key:
                                        HKCU\software\classes\.csh
  Opens key:
                                        HKCR\.csh
  Opens key:
                                        HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
  Opens key:
                                        HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
  Opens kev:
                                        HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\treatas
  Opens key:
                                        HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas
  Opens key:
                                        HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\progid
                                        HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid
  Opens key:
  Opens key:
                                        HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32
                                        HKCR \clsid \final 2d94-0ac9-11d1-896c-00c04fb6bfc4 \clsid \final 2d94-0ac9-11d1-896c-00c04fb6bfc4 \clsid \clsid
  Opens key:
  Opens key:
                                        HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler32
  Opens key:
                                        HKCR \clsid \footnote{Tb8a2d94-0ac9-11d1-896c-00c04fb6bfc4} \label{thkcr} Linprochamdler 32
  Opens key:
                                        HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler
                                        HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler
  Opens key:
  Opens key:
                                        HKLM\system\currentcontrolset\services\crypt32
  Opens key:
                                        HKLM\software\microsoft\windows\currentversion\internet settings
  Opens key:
                                        HKLM\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:
                                        HKLM\software\policies\microsoft\windows\currentversion\internet
settings\
  Opens key:
                                        HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:
                                        HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:
                                        HKLM\software\microsoft\internet explorer\main\featurecontrol
  Opens key:
                                        HKCU\software\microsoft\internet explorer\main\featurecontrol
  Opens key:
                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
  Opens key:
                                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
                                        HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
```

settings\zonemap\domains\

Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\ Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\ HKCU\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zonemap\ranges\ Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_unc\_savedfilecheck HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_unc\_savedfilecheck Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\ HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature zones check zonemap policy kb941001 HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature zones check zonemap policy kb941001 Opens key: HKLM\software\policies Opens key: HKCU\software\policies Opens key: HKCU\software Opens key: HKLM\software HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zonemap Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\zonemap\ranges\ HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\zonemap\protocoldefaults\ Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\domains\ HKLM\software\microsoft\windows\currentversion\internet Opens kev: settings\zonemap\domains\ HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature initialize urlaction shellexecute to allow kb936610 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_initialize\_urlaction\_shellexecute\_to\_allow\_kb936610 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_http\_username\_password\_disable Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_http\_username\_password\_disable Opens kev: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature allow reverse solidus in userinfo kb932562 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_allow\_reverse\_solidus\_in\_userinfo\_kb932562 Opens key: HKLM\software\policies\microsoft\internet explorer Opens key: HKLM\software\policies\microsoft\internet explorer\security Opens key: HKLM\software\microsoft\rpc Opens key:  ${\tt HKLM \ } system \verb|\ current control \ \\ computer name \verb|\ active computer name \ \\$ Opens key: HKLM\system\setup Opens key: HKLM\software\policies\microsoft\windows nt\rpc HKLM\software\policies\microsoft\sqmclient\windows Opens key: Opens key: HKLM\software\microsoft\sqmclient\windows Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\ HKCU\software\microsoft\windows\currentversion\internet settings\zones\0 Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\ Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\ Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\0 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\0 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

HKCU\software\policies\microsoft\windows\currentversion\internet

settings\zones\1
 Opens key: HKLM\software\microsoft\windows\currentversion\internet

settings\zones\1
Opens key:

```
settings\zonemap\
 Opens key:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
 Opens key:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
 Opens key:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\3
 Opens key:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
 Opens key:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
                         HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\
 Opens key:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\0
 Opens key:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
 Opens key:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
 Opens key:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\1
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
 Opens key:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
 Opens key:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\3
                         HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\3
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\3
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\4
                         HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\4
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\4
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
 Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}
 Opens kev:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}\propertybag
 Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}
 Opens kev:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}\propertybag
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\internet settings\zones\0
```

Opens key: HKCU\software\classes\exefile\progid

Opens key: HKCR\exefile\progid

Opens key:

HKLM\software\microsoft\windows\currentversion\shellcompatibility\progids\exefile

Opens key: HKCU\software\classes\exefile\shell\open\ddeexec

Opens key: HKCR\exefile\shell\open\ddeexec

Opens key: HKCU\software\microsoft\windows\currentversion\app paths\schtasks.exe
Opens key: HKLM\software\microsoft\windows\currentversion\app paths\schtasks.exe

Opens key:

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

Opens key:

 $\label{lem:hkcu} HKCU software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \{69d250e4-6c18-11e3-b3bc-806e6f6e6963} \label{lem:hkcu}$ 

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

options\schtasks.exe

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

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

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

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

 $Opens~key: \\ HKCU \setminus software \setminus microsoft \setminus windows~nt \setminus current version \setminus approximately against the property of the property$ 

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

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

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

options Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{69d250e3-6c18-

11e3-b3bc-806e6f6e6963}\

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

Opens key: HKCU\software\classes\appid\schtasks.exe

Opens key: HKCR\appid\schtasks.exe

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

Opens key: HKCU\software\classes\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}

Opens key: HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}
Opens key: HKCU\software\classes\clsid\{0f87369f-a4e5-4cfc-bd3e-

73e6154572dd}\treatas

Opens key:  $HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\treatas$  Opens key:  $HKCU\software\classes\clsid\{0f87369f-a4e5-4cfc-bd3e-}$ 

73e6154572dd}\progid

Opens key: HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\progid Opens key: HKCU\software\classes\clsid\{0f87369f-a4e5-4cfc-bd3e-

73e6154572dd\inprocserver32

Opens key: HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprocserver32

Opens key: HKCU\software\classes\clsid\{0f87369f-a4e5-4cfc-bd3e-

73e6154572dd}\inprochandler32

Opens key:  $\label{eq:hkcr} \mbox{HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\} \mbox{inprochandler32}$ 

Opens key: HKCU\software\classes\clsid\{0f87369f-a4e5-4cfc-bd3e-

73e6154572dd}\inprochandler

Opens key: HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprochandler

Opens key: HKLM\system\currentcontrolset\control\computername
Queries value: HKLM\system\currentcontrolset\control\session

manager[cwdillegalindllsearch]

Queries value:

 $HKLM \verb|\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]|$ 

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

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

Queries 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]

Queries value: HKLM\software\microsoft\windows

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

nt\currentversion\compatibility32[adb62392bc0711707e58e70186cc4ac2]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\windows[loadappinit\_dlls]

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

Queries value:

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

Queries value:

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

Queries value:

Oueries value:

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

Oueries value:

 $HKLM \ software \ microsoft \ \ current version \ \ explorer \ \ folder descriptions \ \ \ \ \ a03a-e3ef65729f3d \ [relative path]$ 

Oueries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{general} a03a-e3ef65729f3d \cal{general} [parsing name]$ 

Oueries value:

 $HKLM \ software \ microsoft \ \ current version \ \ explorer \ \ folder descriptions \ \ \ \ \ a03a-e3ef65729f3d \ [infotip]$ 

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \call{lem:hklm} a03a-e3ef65729f3d \call{lem:hklm} [localized name]$ 

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hklm} a03a-e3ef65729f3d \cal{lem:hklm} [icon]$ 

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hklm} a03a-e3ef65729f3d \soling{ security \so$ 

Queries value:

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

Queries value:

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

Oueries value

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

Queries value:

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

Oueries value:

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

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hklm} a03a-e3ef65729f3d \slights \slight \sligh$ 

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hklm} a03a-e3ef65729f3d \cal{lem:hklm} [publish expanded path]$ 

Oueries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-continuous} HKLM \software \mbox{$3eb685db-65f9-4cf6-a03a-e3ef65729f3d} [initfolder \mbox{$derdescriptions}] \label{thm:local-continuous}$ 

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

folders[appdata]

Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}[category]

Queries value:

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

Oueries value:

Queries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ folder descriptions \ `\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7\} [description]$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-

b744-2eb1ae5198b7}[relativepath]

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \final 14e77-02e7-4e5d-b744-2eb1ae5198b7 \cite{b744-2eb1ae5198b7} \ci$ 

Oueries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ folder descriptions \ `\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7\}[infotip]$ 

Queries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ folder descriptions \ `\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7\} [localized name]$ 

Oueries value:

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}[security]

Queries value:

 $HKLM \ software \ microsoft \ \ current version \ \ \ folder descriptions \ \ \{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7\} \ [stream resource]$ 

Queries value:

 $\label{lem:hklm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7\}[streamresourcetype]$ 

Queries value:

 $HKLM \ software \ microsoft \ vindows \ current version \ explorer \ folder descriptions \ \{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7\} \ [local redirectonly]$ 

Oueries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ folder descriptions \ `\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7\} \ [roamable]$ 

Queries value:

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

Queries value:

 $HKLM \ software \ microsoft \ \ current version \ \ explorer \ \ folder descriptions \ \ \{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7\} \ [stream]$ 

Oueries value:

 $HKLM \ software \ microsoft \ \ current version \ \ explorer \ \ folder descriptions \ \ \{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7\} \ [publish expanded path]$ 

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7\} \ [attributes]$ 

Queries value:

 $HKLM \ software \ microsoft \ vindows \ current version \ explorer \ folder descriptions \ \{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7\} \ [folder type id]$ 

Queries value:

 $HKLM \ software \ `microsoft \ `vindows \ `current version \ `explorer \ folder descriptions \ `\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7\} \ [initfolder handler]$ 

Queries value: HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps] 
Queries value: HKLM\software\microsoft\windows\currentversion\explorer[maximizeapps]

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

08002b30309d}\shellfolder[attributes]

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

08002b30309d}\shellfolder[callforattributes]

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

08002b30309d}\shellfolder[restrictedattributes]

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

08002b30309d}\shellfolder[wantsfordisplay]

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

08002b30309d}\shellfolder[hidefolderverbs]

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

08002b30309d}\shellfolder[usedrophandler]

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

08002b30309d}\shellfolder[wantsforparsing]

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

08002b30309d}\shellfolder[wantsparsedisplayname]

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

08002b30309d}\shellfolder[queryforoverlay]

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

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]

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

08002b30309d}\shellfolder[hideondesktopperuser]

```
HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
 Oueries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
                          HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries value:
08002b30309d}\shellfolder[wantsuniversaldelegate]
                          HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
 Oueries value:
08002b30309d}\shellfolder[nofilefolderjunction]
                          HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
 Oueries value:
08002b30309d}\shellfolder[pintonamespacetree]
 Oueries value:
                          HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hasnavigationenum]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}]
 Queries value:
                          HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
 Oueries value:
\label{thm:linear} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced| [showtypeoverlay] \\ \end{tabular}
 Queries value:
                          HKCR\.exe[]
 Queries value:
                          HKCR\exefile[docobject]
 Queries value:
                          HKCR\systemfileassociations\.exe[docobject]
 Queries value:
                          HKCR\exefile[browseinplace]
 Queries value:
                          HKCR\systemfileassociations\.exe[browseinplace]
 Queries value:
                          HKCR\.exe[content type]
 Queries value:
                          HKCR\exefile[isshortcut]
 Queries value:
                          HKCR\systemfileassociations\.exe[isshortcut]
 Oueries value:
                          HKCR\exefile[alwaysshowext]
 Queries value:
                          HKCR\systemfileassociations\.exe[alwaysshowext]
 Queries value:
                          HKCR\exefile[nevershowext]
 Queries value:
                          HKCR\systemfileassociations\.exe[nevershowext]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[category]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[name]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[parentfolder]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}[description]
 Oueries value:
```

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

b029-7fe99a87c641}[relativepath] Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

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

folders[desktop]

Queries value: HKLM\software\microsoft\com3[com+enabled]

Queries value: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]

Queries value: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[]

Queries value: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprocserver32[threadingmodel]

Queries value: HKLM\software\microsoft\ole[maxsxshashcount]

Queries value:

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

Queries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
Queries value: HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]

Queries value: HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]

Queries value:

 $\label{lem:hklm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}\category\cite{Action}$ 

Queries 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]

Queries value:

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

Queries value:

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

Queries value:

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

b4ef-bd1dc332aeae}[parsingname]

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

 $\label{local-ham} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \fill 158ea5dc-b587-4786-b4ef-bd1dc332aeae \current \$ 

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}]

Queries value:

 $\label{thm:local-prop} $$HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[category]$$ 

Queries value:

 $\label{local-observation} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \eqref{5e6c858f-0e22-4760-9afe-ea3317b67173} \ [name]$ 

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parentfolder]

Queries value:

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

Queries value:

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsingname]

Queries value:

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

Oueries value:

 $\label{localized-microsoft-windows-current-version-explorer-folder-descriptions \ensuremath{$ 5e6c858f-0e22-4760-9afe-ea3317b67173 \ensuremath{$ [localized name] } }$ 

Queries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [icon]$ 

Queries value:

9afe-ea3317b67173}[security] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresource] Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresourcetype] Oueries value: 9afe-ea3317b67173}[localredirectonly] HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[roamable] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[precreate] Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[stream] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[publishexpandedpath] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes] Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[foldertypeid] HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler] Oueries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-2160590473-689474908-1361669368-1002[profileimagepath] Queries value: HKCR\directory[docobject] Queries value: HKCR\folder[docobject] Queries value: HKCR\allfilesystemobjects[docobject] Queries value: HKCR\directory[browseinplace] Queries value: HKCR\folder[browseinplace] Oueries value: HKCR\allfilesystemobjects[browseinplace] Queries value: HKCR\directory[isshortcut] Queries value: HKCR\folder[isshortcut] Queries value: HKCR\allfilesystemobjects[isshortcut] Queries value: HKCR\directory[alwaysshowext] Oueries value: HKCR\directory[nevershowext] Queries value: HKCR\folder[nevershowext] Queries value: HKCR\allfilesystemobjects[nevershowext] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\kindmap[.exe] Oueries value: HKLM\system\currentcontrolset\control\cmf\config[system] Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable] Queries value: HKCR\exefile[nostaticdefaultverb] Queries value: HKCR\exefile\shell[] Queries value: HKCR\exefile\shell\open[neverdefault] Queries value: HKCR\exefile\shell\open\command[delegateexecute] Queries value: HKCR\.asp[] Queries value: HKCR\.bas[] Queries value: HKCR\.bat[] HKCR\.cer[] Oueries value: Queries value: HKCR\.chm[] Queries value: HKCR\.cmd[] Queries value: HKCR\.com[] Queries value: HKCR\.cpl[] Queries value: HKCR\.crt[] Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[] Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[inprocserver32] HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[] Oueries value: Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[threadingmodel] Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags] Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[disableimprovedzonecheck]

HKLM\software\policies\microsoft\windows\currentversion\internet

Queries value: HKLM\software\microsoft\internet

Oueries value:

settings[security\_hklm\_only]

```
explorer\main\featurecontrol\feature_unc_savedfilecheck[adb62392bc0711707e58e70186cc4ac2.exe]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[*]
 Queries value:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
 Queries value:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
 Queries value:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
 Queries value:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
                         HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_http_username_password_disable[adb62392bc0711707e58e70186cc4ac2.exe]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[*]
                         HKLM\software\policies\microsoft\internet
 Queries value:
explorer\security[disablesecuritysettingscheck]
                         HKLM\software\microsoft\rpc[maxrpcsize]
 Queries value:
 Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
                         HKLM\system\setup[oobeinprogress]
 Queries value:
 Queries value:
                         HKLM\system\setup[systemsetupinprogress]
 Queries value:
                         HKLM\software\microsoft\sqmclient\windows[ceipenable]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[flags]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[flags]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[flags]
                         HKCU\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[adb62392bc0711707e58e70186cc4ac2.exe]
                         HKCU\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
 Oueries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature localmachine lockdown[adb62392bc0711707e58e70186cc4ac2.exe]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
                         HKLM\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[specialfolderscachesize]
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[specialfolderscachesize]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[specialfolderscachesize]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
 Queries value:
ba85-6007caedcf9d}[category]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[name]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[parentfolder]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[description]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[relativepath]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[parsingname]
```

Queries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ folder descriptions \ `\{352481e8-33be-4251-ba85-6007 caed \ folder \ fol$ 

Queries value:

 $HKLM \ software \ microsoft \ vurrent version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ folder \ descriptions \ folder \ folder \ descriptions \ folder \ fol$ 

Oueries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ folder descriptions \ `\{352481e8-33be-4251-ba85-6007 caed \ folder \ fol$ 

Queries value:

 $HKLM \ software \ microsoft \ vurrent version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ folder \$ 

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caedcf9d\} [stream resource]$ 

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresourcetype]

Queries value:

 $HKLM \ software \ microsoft \ \ current version \ \ explorer \ folder descriptions \ \ \{352481e8-33be-4251-ba85-6007 caed \ folder \ \ descriptions \ \ \ \} \ [local redirectionly]$ 

Queries value:

 $HKLM \ software \ microsoft \ vurrent version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ folder \$ 

Oueries value:

 $\label{lem:hklm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d\}[precreate]$ 

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hklm} as 5-6007 \caed \cal{lem:hklm} folder \cal{lem:hklm} as 5-6007 \caed \cal{lem:hklm} as 5-6007 \caed \cal{lem:hklm} as 6-6007 \caed \ca$ 

Queries value:

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

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{local-quantum} \footnote{1.5} attributes \cal{local-quantum-q$ 

Queries value:

Queries value:

 $\label{thm:local-continuous} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \colored \colored \folder \f$ 

Queries value:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \user shell \end{tabular}$ 

folders[cache]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[category]

Queries value:

 $HKLM \ software \ microsoft \ vindows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ [name]$ 

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \eqref{2b0f765d-c0e9-4171-908e-08a611b84ff6} \cite{Conditions} \cite{Con$ 

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ [description]$ 

Queries value:

 $HKLM \ software \ microsoft \ \ current version \ \ explorer \ \ folder descriptions \ \ \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [relative path]$ 

Queries value:

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[infotip]

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \calebox{2b0f765d-c0e9-4171-908e-08a611b84ff6} [localized name]$ 

Queries value:

 $\label{local-observation} \begin{tabular}{l} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \current version \explorer \explore$ 

Queries value:

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

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[streamresource]

Queries value:

908e-08a611b84ff6}[streamresourcetype]

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[localredirectonly]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[roamable]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[precreate]

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[stream]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[publishexpandedpath]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[attributes]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-d0e7de8d-c0e9-$ 908e-08a611b84ff6}[foldertypeid]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[initfolderhandler]

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

folders[cookies]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature\_protocol\_lockdown[adb62392bc0711707e58e70186cc4ac2.exe]

Oueries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_protocol\_lockdown[\*]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\zones\0[1806]

Queries value: HKLM\software\microsoft\windows\currentversion\internet

settings\zones\0[1806]

Queries value: HKCR\exefile\shell\open\command[command]

HKCR\exefile\shell\open\command[] Queries value:

Queries value: HKCR\exefile\shell\open[setworkingdirectoryfromtarget]

Queries value: HKCR\exefile\shell\open[noworkingdirectory]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{69d250e4-6c18-11e3-b3bc-806e6f6e6963}[data]

Queries value:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mountpoints 2 \setminus cpc \setminus volume \setminus \{69d250e4-6c18-explorer\} \setminus (69d250e4-6c18-explorer) \setminus$ 11e3-b3bc-806e6f6e6963}[generation]

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

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]

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

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{69d250e3-6c18-11e3-b3bc-806e6f6e6963}[data]

Queries value:

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

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

manager[pendingfilerenameoperations2]

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

manager[pendingfilerenameoperations]

HKLM\software\microsoft\windows Oueries value:

nt\currentversion\compatibility32[schtasks]

Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist] Oueries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]

Queries value: HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\progid[]

Queries value: HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}[]

Queries value: HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-

73e6154572dd}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprocserver32[] Queries value: HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-

73e6154572dd}\inprocserver32[threadingmodel]

Sets/Creates value: HKLM\system\currentcontrolset\control\session

manager[pendingfilerenameoperations]

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap[uncasintranet]

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap[autodetect]