Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 129, Task ID: 517

Task ID: 517

Risk Level: 6

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

Processing Time: 3.55 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\SysWOW64\schtasks.exe ["C:\Windows\SysWOW64\schtasks.exe"

/Delete /TN EPUpdater /F]

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

Terminates process: C:\Windows\SysWOW64\schtasks.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
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-0x000000000000890
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

Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\System32\wow64win.dll
Opens: C:\Windows\System32\wow64cpu.dll
Opens: C:\Windows\system32\wow64log.dll

Opens: C:\Windows\SysWOW64

Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\Windows\SysWOW64\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\SysWOW64\rpcss.dl1
Opens: C:\Windows\SysWOW64\uxtheme.dl1
Opens: C:\Windows\SysWOW64\schtasks.exe
Opens: C:\windows\temp\PROPSYS.dl1
Opens: C:\Windows\SysWOW64\propsys.dl1
Opens: C:\Windows\SysWOW64\shell32.dl1

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\SysWOW64\ntmarta.dll

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

4C77-AF34-C647E37CA0D9}.1.ver0x000000000000001.db

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

Opens: C:\windows\temp\profapi.dll
Opens: C:\Windows\SysWOW64\profapi.dll
Opens: C:\Windows\System32\propsys.dll

Opens: C:\Windows\SysWOW64\en-US\propsys.dll.mui

Opens: C:\Windows\SysWOW64\urlmon.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\SysWOW64\schtasks.exe:Zone.Identifier
Opens: C:\Windows\SysWOW64\en-US\setupapi.dll.mui

Opens: C:\Windows\SysWOW64\apphelp.dll
Opens: C:\Windows\AppPatch\sysmain.sdb
Opens: C:\Windows\SysWOW64\ui\SwDRM.dll

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

Opens: C:\Windows\Prefetch\SCHTASKS.EXE-AD598958.pf

Opens: C:\Windows\SysWOW64\ktmw32.dll

Opens: C:\Windows\SysWOW64\en-US\schtasks.exe.mui

Opens: C:\Windows\SysWOW64\version.dll
Opens: C:\Windows\SysWOW64\taskschd.dll

Opens: C:\Windows\SysWOW64\en-US\KernelBase.dll.mui

Reads from: C:\Users\Admin\Desktop\desktop.ini
Reads from: C:\Windows\Sys\WO\M64\schtasks.exe

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\wow6432node\microsoft\windows\currentversion\internet

settings\zonemap[proxybypass]

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

settings\zonemap[intranetname]

Deletes value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\zonemap[intranetname]

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

options

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

Opens key: HKLM\software\microsoft\wow64

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

execution options

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

Opens key:

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

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

Opens key: HKLM\system\currentcontrol\set\control\nls\customlocale
Opens key: HKLM\system\currentcontrol\set\control\nls\language
Opens key: HKLM\system\currentcontrol\set\control\mui\uilanguages
Opens key: HKLM\system\currentcontrol\set\control\mui\uilanguages\en-us

 $Opens~key: \\ \hspace*{0.2cm} HKLM\system\current control set\control\ mui\ uilanguages\ pending delete$

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

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

Opens key: HKCU\

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

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

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

 $Opens~key: \\ \qquad \qquad \text{HKLM} software \\ \\ \text{wow} 6432 \\ \text{node} \\ \\ \text{microsoft} \\ \\ \text{windows} \\ \\ \text{current} \\ \text{version} \\ \\ \text{side} \\ \text{byside} \\ \\ \text{opens} \\ \\ \text{key} \\ \\ \text{opens} \\ \\ \text{the lowest} \\ \\ \text{opens} \\ \\ \text{the lowest} \\ \\ \text{opens} \\ \\ \text{o$

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

Opens key: HKLM\

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

 $\verb|nt\currentversion\diagnostics||$

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

nt\currentversion\gre_initialize

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32

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

compatibility

HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows

Opens key:

 $Opens \ key: \\ HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ de$

Opens kev: HKLM\software\wow6432node\microsoft\ole

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

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

Opens key:

 $\label{lem:hklm} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \calebox{3eb685db-65f9-4cf6-a03a-e3ef65729f3d} \\$

Opens key

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

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

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

Opens key:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \session in folders \end{tabular} \label{lem:hkcu}$

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

folders

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

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings

Opens key:

b2f1-4857-a4ce-a8e7c6ea7d27}

Opens key:

b2f1-4857-a4ce-a8e7c6ea7d27}\propertybag

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ adb 62392 bc 0711707e58e70186cc4ac2. exemple \ according to the compatibility \ applications \ adb 62392 bc 0711707e58e70186cc4ac2. exemple \ according to the compatibility \ applications \ adb 62392 bc 0711707e58e70186cc4ac2. exemple \ according to the compatibility \ according to$

Opens key: $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus explorer$

Opens key:

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

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

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

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side \ as sembly storage roots$

Opens key: HKCU\software\classes\

Opens key: HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder

HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Opens key:

08002b30309d}\shellfolder

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\clsid| {20d04fe0-properties of the context of the$ Opens key:

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

Opens kev:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-

a2d8-08002b30309d}\shellfolder

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

Opens key:

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum \setminus microsoft \setminus windows \setminus current version \setminus microsoft \setminus windows \setminus current version \setminus microsoft \setminus$

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

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

 $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ advanced$ Opens key:

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 HKCU\software\microsoft\windows\currentversion\explorer\fileexts Opens key: Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\fileexts|.exe| \\ \end{tabular}$ 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

HKCR\exefile\shellex\iconhandler Opens key:

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

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

Opens key: HKCR\exefile\browseinplace

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

Opens key: HKCR\systemfileassociations\.exe\browseinplace

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

Opens key: HKCR\exefile\clsid

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

Opens kev:

db2c-424c-b029-7fe99a87c641}

Opens key:

db2c-424c-b029-7fe99a87c641}\propertybag

HKLM\software\microsoft\com3

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

b8dc300d9f9d}

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

b8dc300d9f9d}\treatas

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

b8dc300d9f9d}\progid

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

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

b8dc300d9f9d}\progid

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

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler32

Opens key:

b8dc300d9f9d}\inprochandler

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

b8dc300d9f9d}\inprochandler

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

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

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1b3ea5dc-b2b4a2b4b2ab4b2a2$

b587-4786-b4ef-bd1dc332aeae}

Opens kev:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-part \ and \ barrier \ barr$

b587-4786-b4ef-bd1dc332aeae}\propertybag

Opens key:

0e22-4760-9afe-ea3317b67173}

Opens key:

0e22-4760-9afe-ea3317b67173}\propertybag

HKLM\software\wow6432node\microsoft\windows nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001

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

980053277-1733835069-2361817685-1001

Opens key:

 $HKLM \label{lem:hklm} Which is the last of the last$

Opens key:

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

HKCU\software\classes\directory Opens key:

Opens key: HKCR\directory

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

HKCR\directory\curver Opens key: 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

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

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 kev: HKCU\software\classes\folder\docobject

Opens key: HKCR\folder\docobject

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

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:
                          HKCU\software\classes\allfilesystemobjects\clsid
 Opens key:
                          HKCR\allfilesystemobjects\clsid
 Opens key:
                          HKLM\software\microsoft\windows\currentversion\explorer\kindmap
 Opens key:
                          HKLM\system\currentcontrolset\control\cmf\config
 Opens key:
                          HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
 Opens kev:
                          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\
 Opens key:
                          HKCU\software\classes\exefile\shell\open\command
 Opens key:
                          HKCR\exefile\shell\open\command
 Opens key:
                          HKCU\software\classes\exefile\shell\open\droptarget
 Opens key:
                          HKCR\exefile\shell\open\droptarget
 Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ policies \ associations
 Opens key:
                          HKLM\software\microsoft\windows\currentversion\policies\associations
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\policies\associations
 Opens key:
                          HKCU\software\classes\.ade
                          HKCR\.ade
 Opens kev:
 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
 Opens key:
                          HKCU\software\classes\.bat
 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
                          HKCU\software\classes\.com
 Opens key:
 Opens key:
                          HKCR\.com
 Opens key:
                          HKCU\software\classes\.cpl
 Opens key:
                          HKCR\.cpl
 Opens key:
                          HKCU\software\classes\.crt
 Opens key:
                          HKCR\.crt
 Opens key:
                          HKCU\software\classes\.csh
 Opens key:
                          HKCR\.csh
 Opens key:
                          HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}
 Opens key:
                          HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
 Opens key:
                          HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\treatas
 Opens key:
                          HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas
 Opens key:
                          HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\progid
 Opens key:
                          HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid
                          HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
 Opens key:
 Opens key:
                          HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
 Opens key:
                          HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\progid
 Opens key:
                          HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid
 Opens key:
                          HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32
                          HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-1}
 Opens key:
00c04fb6bfc4}\inprocserver32
 Opens key:
                          HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler32
                          HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
 Opens key:
00c04fb6bfc4}\inprochandler32
 Opens key:
                          HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler
                          HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
 Opens key:
00c04fb6bfc4}\inprochandler
 Opens key:
                          HKLM\system\currentcontrolset\services\crypt32
 Opens key:
                          HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet
settings
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings
```

Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\ Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\main\featurecontrol Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol HKCU\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 Opens kev: settings\zonemap\domains\ $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} on the constraint of the$ Opens key: settings\zonemap\domains HKCU\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zonemap\domains\ Opens key: settings\zonemap\ranges\ $\label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ Opens kev: settings\zonemap\ranges HKCU\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\zonemap\ranges\ Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck HKLM\software\wow6432node\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\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001 Opens key: HKLM\software\wow6432node\policies Opens key: HKCU\software\policies Opens key: HKCU\software Opens key: HKLM\software\wow6432node Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap Opens key: $\label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ settings Opens kev: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\zonemap\ranges\ $\label{thm:linear} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet}}$ Opens key: settings\zonemap\protocoldefaults\ Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\domains\ Opens key: $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version\\| internet$ settings\zonemap\domains\ HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610 HKCU\software\microsoft\windows\currentversion\internet settings Opens key: Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_http_username_password_disable HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature_http_username_password_disable HKCU\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562 Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer Opens kev:

HKLM\software\policies\microsoft\internet explorer

Opens key: HKLM\software\policies\microsoft\internet explorer\security

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

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

Opens key: HKLM\system\setup

 $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM\software\wow6432node\policies\microsoft\windows\ nt\rpc \end{tabular}$ Opens key:

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

```
Opens key:
                           HKLM\software\microsoft\sqmclient\windows
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
 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\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\
 Opens key:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones
 Opens kev:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\0
                           HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\zones\0
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\1
 Opens key:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
                           HKI M\software\wow6432node\microsoft\windows\currentversion\internet
 Opens key:
settings\zonemap\
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\2
                           HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\2
                           \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
 Opens key:
settings\zones\2
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\3
 Opens key:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
 Opens kev:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\4
 Opens key:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\4
 Opens key:
                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
 Opens key:
                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
 Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\lockdown_zones\
 Opens key:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
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 kev:
settings\lockdown_zones\0
 Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\lockdown_zones\0
                           HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\0
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                           HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown zones\1
 Opens key:
HKLM\software\wow6432node\policies\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 \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
```

settings\lockdown_zones\2

```
HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\2
   Opens key:
                                                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown zones\2
   Opens key:
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
   Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\lockdown_zones\3
                                                 HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\3
   Opens key:
                                                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\4
   Opens kev:
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 kev:
settings\lockdown_zones\4
                                                 HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
                                                 HKLM\software\wow6432node\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
   Opens key:
HKLM \label{lem:hklm} Which is the latest and the
33be-4251-ba85-6007caedcf9d}
   Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{352481e8-1644444 \ explorer \ folder \ explorer \ \ \}
33be-4251-ba85-6007caedcf9d}\propertybag
c0e9-4171-908e-08a611b84ff6}
   Opens key:
c0e9-4171-908e-08a611b84ff6}\propertybag
                                                 HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_protocol_lockdown
   Opens key:
                                                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
                                                 HKLM\software\wow6432node\microsoft\windows\currentversion\internet
   Opens key:
settings\zones\0
   Opens key:
                                                 HKCU\software\classes\exefile\progid
   Opens key:
                                                 HKCR\exefile\progid
   Opens key:
Opens key:
                                                 HKCU\software\classes\exefile\shell\open\ddeexec
                                                 HKCR\exefile\shell\open\ddeexec
   Opens key:
   Opens key:
                                                 HKCU\software\microsoft\windows\currentversion\app paths\schtasks.exe
   Opens key:
                                                 HKLM\software\wow6432node\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:
11e3-a68e-806e6f6e6963}\
                                                 HKLM\software\wow6432node\microsoft\windows\currentversion\setup
   Opens key:
   Opens key:
                                                 HKLM\software\wow6432node\microsoft\windows\currentversion
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-
11e3-a68e-806e6f6e6963}\
   Opens key:
                                                 \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\schtasks.exe
   Opens key:
                                                 HKLM\system\currentcontrolset\control\session manager\appcertdlls
   Opens key:
                                                 HKLM\system\currentcontrolset\control\session manager\appcompatibility
   Opens key:
                                                 HKLM\software\wow6432node\policies\microsoft\windows\appcompat
   Opens key:
                                                 HKLM\software\policies\microsoft\windows\appcompat
   Opens key:
                                                 HKCU\software\microsoft\windows\currentversion\explorer\shell folders
   Opens key:
                                                 \label{lem:hklm} \mbox{HKLM} \mbox{$\tt MKLM} \mbox
   Opens key:
                                                 HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
                                                 HKLM\software\microsoft\windows
   Opens kev:
nt\currentversion\appcompatflags\custom\schtasks.exe
   Opens key:
                                                 HKLM\system\currentcontrolset\control\samservicelist
   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\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-
```

73e6154572dd}

Opens key: HKCR\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd\}
Opens key: HKCU\software\classes\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-

73e6154572dd}\treatas

 $\label{thm:continuous} Opens~key: $$ HKCR\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\treatas $$ Opens~key: $$ HKCU\software\classes\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\treatas $$ Opens~key: $$ HKCU\software\classes\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\treatas $$ Opens~key: $$ HKCU\software\classes\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\treatas $$ Opens~key: $$

73e6154572dd}\progid

Opens key: HKCR\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\progid Opens key: HKCU\software\classes\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-

73e6154572dd}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-

73e6154572dd}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-

73e6154572dd}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-

73e6154572dd}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-

73e6154572dd}\inprochandler

Opens key: HKCR\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-

73e6154572dd}\inprochandler

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

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

options[disableusermodecallbackfilter]

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

manager[cwdillegalindllsearch]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]

Queries value:

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

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

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

us[alternatecodepage]

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

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

Queries value:

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

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

Queries value: HKLM\system\currentcontrol\session manager[safedllsearchmode]

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

Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[adb62392bc0711707e58e70186cc4ac2]
Queries value: HKLM\software\wow6432node\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 \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:condition} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fold$

Oueries value

 $\label{thm:hammon} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \folder$

Queries value:

 $\label{limit} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder 65f9-4cf6-a03a-e3ef65729f3d\folder\fo$

Queries value:

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

Oueries value:

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

Oueries value

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

Oueries value:

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

Queries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder 6569-4cf6-a03a-e3ef65729f3d\folder 6569-4$

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value

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

Queries value

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

Queries value:

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

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

folders[appdata]

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

Queries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27\} \ [name]$

Oueries value:

 $\label{limit} \begin{tabular}{ll} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fold$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27\} [description]$

Queries value:

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}[parsingname]

Queries value:

 $\label{limits} $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27\}[infotip]}$

Oueries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27\} \ [localized name]$

Oueries value:

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

Oueries value:

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\def{hklmsoftware} d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27\}[streamresource]$

Queries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27\} [stream resource type]$

Queries value:

 $\label{localization} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \end{de5231b0-b2f1-4857-a4ce-a8e7c6ea7d27} \[local redirectonly]$

Oueries value:

 $\label{local-hklm} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \explorer \folder descriptions \folder \folder$

Queries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}[precreate]

Queries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27\} [stream]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27\} \ [publish expanded path]$

Queries value:

```
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d
b2f1-4857-a4ce-a8e7c6ea7d27}[attributes]
   Queries value:
HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{d65231b0-d1014\} \\ descriptions \setminus \{d6524b0-d1014\} \\ descriptions \setminus \{d654b0-d1014\} \\
b2f1-4857-a4ce-a8e7c6ea7d27}[foldertypeid]
   Oueries value:
b2f1-4857-a4ce-a8e7c6ea7d27}[initfolderhandler]
   Oueries value:
                                                    HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer[maximizeapps]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[enableshellexecutehooks]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
   Oueries value:
                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[callforattributes]
                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[restrictedattributes]
   Queries value:
                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsfordisplay]
                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[hidefolderverbs]
   Oueries value:
                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[usedrophandler]
   Oueries value:
                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsforparsing]
                                                    Oueries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[queryforoverlay]
                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[mapnetdriveverbs]
                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[queryforinfotip]
   Queries value:
                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideinwebview]
                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[hideondesktopperuser]
                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
   Queries value:
                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsuniversaldelegate]
   Queries value:
                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[nofilefolderjunction]
                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[pintonamespacetree]
   Oueries value:
                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hasnavigationenum]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}1
   Queries value:
                                                    HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
   Queries value:
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
```

Oueries 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] Oueries value:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{lem:hkcu} advanced \cite{lem:$

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

Queries value:

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

Oueries value:

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

Oueries value:

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

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

Queries value:

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

Oueries value:

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

Oueries value:

Queries value:

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

Oueries value:

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

Queries value:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{tabular} is a constant \cite{tabular} and \cite{tabular$

HKCR\.exe[] Queries value:

Queries value: HKCR\exefile[docobject]

Queries value: HKCR\systemfileassociations\.exe[docobject]

Queries value: HKCR\exefile[browseinplace]

HKCR\systemfileassociations\.exe[browseinplace] Oueries value:

Queries value: HKCR\.exe[content type] Oueries value: HKCR\exefile[isshortcut]

Oueries value: HKCR\systemfileassociations\.exe[isshortcut]

Queries value: HKCR\exefile[alwaysshowext]

Oueries value: HKCR\systemfileassociations\.exe[alwaysshowext]

HKCR\exefile[nevershowext] Queries value:

Oueries value: HKCR\systemfileassociations\.exe[nevershowext]

Queries value:

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

Oueries value:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{b4bfcc3a-b4bf$ db2c-424c-b029-7fe99a87c641}[name]

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3adb2c-424c-b029-7fe99a87c641}[security]

Queries value:

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

Oueries value:

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

Oueries value:

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

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

Queries value:

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

Queries value:

 $\label{limit} \begin{tabular}{ll} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fold$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3adb2c-424c-b029-7fe99a87c641\} \ [publish expanded path]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3adb2c-424c-b029-7fe99a87c641\} [attributes]$

Oueries value:

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

Oueries value:

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

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

folders[desktop]

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

Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]

Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprocserver32[]

Queries value: HKCR\wow6432node\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]

Oueries value:

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(1b3ea5dc-b587-4786-b4ef-bd1dc332aeae)\cite{lem:hklmsoftware}\cite{lem:hklmsoftw$

Queries value:

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

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(1b3ea5dc-b587-4786-b4ef-bd1dc332aeae)\f(relative path)\f(relative path)\f(relative$

Queries value:

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

Queries value:

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

Oueries value:

Queries value:

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

Queries value

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

Queries value:

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

Oueries value:

 $\label{thm:local-bound} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[streamresourcetype]}$

Queries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[localredirectonly]

Queries value

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value

 $\label{thm:local-holes} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1} \footnote{2} \footnote{2$

Queries value:

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

Oueries value:

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

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

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

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1}{2} each \footnote{1$

Oueries value

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

Queries value:

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

Oueries value:

 $\label{thm:local-ham} $$HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[description]}$

Queries value:

 $\label{thm:local-ham} $$HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[relativepath]}$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [parsing name]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [infotip]$

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [icon]$

Oueries value:

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

Queries value:

 $\label{thm:local-ham} $$HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[streamresource]$$

Queries value:

 $\label{limits} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[streamresourcetype]}$

Queries value:

 $\label{thm:local-continuous} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fold$

Queries value:

 $\label{thm:local-hammon} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \$

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-ham} $$HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[publishexpandedpath]$

Oueries value

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[attributes]$

Queries value:

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

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler]

Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

980053277-1733835069-2361817685-1001[profileimagepath]
Queries value: HKCR\directory[docobject]

Queries value: HKCR\folder[docobject]

Queries value: HKCR\allfilesystemobjects[docobject]

```
HKCR\directory[browseinplace]
 Oueries value:
 Oueries value:
                          HKCR\folder[browseinplace]
 Queries value:
                          HKCR\allfilesystemobjects[browseinplace]
 Queries value:
                          HKCR\directory[isshortcut]
 Queries value:
                          HKCR\folder[isshortcut]
 Queries value:
                          HKCR\allfilesystemobjects[isshortcut]
 Oueries value:
                          HKCR\directory[alwaysshowext]
                          HKCR\directory[nevershowext]
 Queries value:
 Oueries 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\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
 Queries value:
                          HKCR\exefile[nostaticdefaultverb]
                          HKCR\exefile\shell[]
 Oueries value:
 Queries value:
                          HKCR\exefile\shell\open[neverdefault]
 Queries value:
                          HKCR\exefile\shell\open\command[delegateexecute]
                          HKCR\.asp[]
 Oueries value:
 Queries value:
                          HKCR\.bas[]
 Oueries value:
                          HKCR\.bat[]
 Queries value:
                          HKCR\.cer[]
 Queries value:
                          HKCR\.chm[]
 Queries value:
                          HKCR\.cmd[]
 Queries value:
                          HKCR\.com[]
 Oueries value:
                          HKCR\.cpl[]
 Queries value:
                          HKCR\.crt[]
                          HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[]
 Oueries value:
 Queries value:
                          HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[inprocserver32]
                          HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
 Queries value:
00c04fb6bfc4}\inprocserver32[]
                          HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
 Oueries value:
00c04fb6bfc4}\inprocserver32[threadingmodel]
                          HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
 Oueries value:
 Oueries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
 Queries value:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[adb62392bc0711707e58e70186cc4ac2.exe]
 Queries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[*]
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[createuricachesize]
 Queries value:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[createuricachesize]
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablepunycode]
 Queries value:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
 Queries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[adb62392bc0711707e58e70186cc4ac2.exe]
 Queries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[*]
 Queries value:
                          HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
                          HKLM\software\microsoft\rpc[maxrpcsize]
 Oueries value:
 Queries value:
HKLM\system\currentcontrol\set\control\computername[computername]
 Queries value:
                          HKLM\system\setup[oobeinprogress]
 Oueries value:
                          HKLM\system\setup[systemsetupinprogress]
                          HKLM\software\microsoft\sqmclient\windows[ceipenable]
 Oueries value:
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\1[flags]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\2[flags]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\3[flags]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[flags]
 Queries value:
                          HKCU\software\microsoft\internet
\verb|explorer| a in feature control feature_local machine_lockdown[adb62392bc0711707e58e70186cc4ac2.exe]| \\
```

Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[*] Queries value: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature localmachine lockdown[adb62392bc0711707e58e70186cc4ac2.exe]

Queries value: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_localmachine_lockdown[*]

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

settings[specialfolderscachesize]

 $Queries \ value: \\ HKCU \ software \ policies \ microsoft \ windows \ current version \ internet$

settings[specialfolderscachesize]

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

settings[specialfolderscachesize]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings[specialfolderscachesize]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ folder \ f$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ folder \ f$

Oueries value:

 $\label{thm:local-base-bound} HKLM software \noinder local-base-6007 caed cf9d [parent folder] \\$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ folder \ f$

Queries value

 $\label{thm:local-ham} $$HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}\[relative\path]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caedcf9d\} \ [parsing name]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ folder \ f$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caedcf9d\} \ [localized name]$

Queries value:

 $\label{thm:local-base-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folds \folds$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1} as be-4251-ba85-6007 caed \cf9d \cfg [security]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ folder \ f$

Queries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresourcetype]

Queries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ folder \ f$

Queries value:

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

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cal{lem:hklmsoftware} \end{substitute} 33be-4251-ba85-6007\caedcf9d\cal{lem:hklmsoftware} [precreate]$

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\calebox{352481e8-33be-4251-ba85-6007} [stream]$

Queries value

 $\label{thm:local-base-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1}{352481e8-33be-4251-ba85-6007} caed \cf9d \cf{publish} publish \expanded \cpand \cf{publish} and \cf{pu$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ folder \ f$

Oueries value:

 $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007} [foldertypeid]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ folder \ handler]$

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

folders[cache]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ [category]$

Oueries value:

c0e9-4171-908e-08a611b84ff6}[name]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ [parentfolder]$

Queries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[description]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [relative path]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [parsing name]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ [infotip]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ [localized name]$

Queries value

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \cdot \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \cdot \cdot\cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [security]$

Oueries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[stream resource type]$

Oueries value

 $\label{local_ham} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\cdots\$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ [roamable]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ for exercise \ for example \ for e$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[stream]$

Oueries value

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

Queries value:

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

Queries value:

 $\label{limits} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\coe9-4171-908e-08a611b84ff6\folder\coe9-4171-908e-$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [initfolder \ handler]$

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

folders[cookies]

Queries value: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_protocol_lockdown[adb62392bc0711707e58e70186cc4ac2.exe]

Queries value: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_protocol_lockdown[*]

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

settings\zones\0[1806]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\zones\0[1806]

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

Oueries value:

 $\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} A microsoft \end{tabular} windows \end{tabular} explorer [inherit consoleh and les]$

Queries value:

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

Queries value:

HKLM\software\microsoft\windows\currentversion\policies\explorer[disallowrun]
 Queries value: HKCR\exefile\shell\open[setworkingdirectoryfromtarget]

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

Queries value:

 $\label{lem:hkculsoftware} HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d4-8213-11e3-a68e-806e6f6e6963}\ [data]$

Oueries value:

 $HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ \{8063a3d4-8213-11e3-a68e-806e6f6e6963\} \cite{Microsoft} \end{substitute}$

 $\label{thm:linear} Queries \ value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath] \\ Queries \ value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath] \\$

Queries value:

 $\label{thm:local-condition} HKCU software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ \{8063a3d3-8213-11e3-a68e-806e6f6e6963\} \ [data]$

Oueries value:

 $\label{thm:local-continuous} HKCU software \\ \min cosoft \\ \min cosoft \\ \min explorer \\ 11e3-a68e-806e6f6e6963\\ [generation]$

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[cache]

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

options[disablelocaloverride]

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

manager[pendingfilerenameoperations2]

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

manager[pendingfilerenameoperations]

Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\compatibility32[schtasks]

Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
Queries value: HKCR\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\progid[]
Queries value: HKCR\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}[]

Queries value: HKCR\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e615}

Queries value: HKCR\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-

Queries value: HKCR\wow6432node\clsid\{ 73e6154572dd}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{0f87369f-a4e5-4cfc-bd3e-

73e6154572dd}\inprocserver32[]

Queries value: HKCR\wow6432node\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]