Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 129, Task ID: 514

Task ID: 514

Risk Level: 6

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

Processing Time: 3.35 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]

Creates process: \SystemRoot\System32\Conhost.exe [\??\C:\Windows\system32\conhost.exe

0xffffffff]

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

Terminates process: C:\Windows\Sys\W0\64\schtasks.exe
Terminates process: C:\Windows\System32\conhost.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

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

File System Events

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

Opens: C:\Windows

Opens: C:\Windows\System32\wow64.dll

Opens: C:\Windows\SysW0W64

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

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

Opens: C:\Windows\SvsWOW64\ntdll.dll Opens: C:\Windows\SysWOW64\kernel32.dll C:\Windows\SysWOW64\KernelBase.dll Opens: Opens: C:\Windows\apppatch\sysmain.sdb C:\Windows\SysWOW64\sechost.dll Opens: C:\Windows\SysWOW64\combase.dll Opens: Opens: C:\Windows\SysWOW64\msvcrt.dll C:\Windows\SysWOW64\gdi32.dll Opens: C:\Windows\SysWOW64\user32.dll Opens: C:\Windows\SysWOW64\shlwapi.dll Opens:

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

Opens: C:\Windows\SysWOW64\cryptbase.dll C:\Windows\SysWOW64\sspicli.dll Opens: Opens: C:\Windows\SysWOW64\rpcrt4.dll Opens: C:\Windows\SysWOW64\advapi32.dll C:\Windows\SysWOW64\shell32.dll Opens: C:\Windows\SysWOW64\imm32.dll Opens: C:\Windows\SysWOW64\msctf.dll Opens: Opens: C:\Windows\SysWOW64\SHCore.dll

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

Opens: C:\Windows\SysWOW64\uxtheme.dll
Opens: C:\Windows\SysWOW64\ole32.dll
Opens: C:\Windows\SysWOW64\oleaut32.dll
Opens: C:\Windows\SysWOW64\propsys.dll
Opens: C:\Windows\SysWOW64\clbcatq.dll

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

4C77-AF34-C647E37CA0D9}.1.ver0x000000000000000e.db

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

C:\Windows\SysWOW64\profapi.dll Opens: Opens: C:\Windows\SysWOW64\urlmon.dll Opens: C:\Windows\SysWOW64\iertutil.dll Opens: C:\Windows\SysWOW64\wininet.dll Opens: C:\Windows\SysWOW64\secur32.dll Opens: C:\ Opens: C:\Windows\SysWOW64\schtasks.exe Opens: C:\Windows\SysWOW64\cfgmgr32.dll C:\Windows\SysWOW64\devobj.dll Opens: C:\Windows\SysWOW64\setupapi.dll Opens: Opens: C:\Windows\Prefetch\SCHTASKS.EXE-AD598958.pf C:\Windows\System32\conhost.exe Opens:

Opens: C:\Windows\system32\combase.dll

Opens: C:\Windows\WinSxS\amd64_microsoft.windows.common-

Opens: C:\Windows\WindowsShell.Manifest
Opens: C:\Windows\System32\SHCore.dll
Opens: C:\Windows\SysWOW64\ktmw32.dll
Opens: C:\Windows\SysWOW64\version.dll
Opens: C:\Windows\SysWOW64\taskschd.dll
Reads from: C:\Users\Admin\Desktop\desktop.ini
Reads from: C:\Windows\SysWOW64\schtasks.exe

Windows Registry Events

Creates key: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap\

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\wow64

 $\label{lem:control} Opens~key: $$ HKLM\system\currentcontrolset\control\safeboot\option $$ Opens~key: $$ HKLM\system\currentcontrolset\control\srp\gp\dll $$$

Opens key:

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

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\currentcontrolset\control\nls\language

Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages

Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us

Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete

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

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

Opens key: HKCU\

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

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

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

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

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

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

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

 $Opens \ key: \\ HKLM \ software \ microsoft \ windows \\ nt \ current version \ app compatflags \ disable 8 and 16 bit mitigation \\$

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

nt\currentversion\gre_initialize

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

nt\currentversion\compatibility32

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

compatibility

Opens key: HKLM\

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

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

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

Opens key:

HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration

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

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

Opens key:

Opens kev:

65f9-4cf6-a03a-e3ef65729f3d}

Opens key:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685db-16422 \\ node \setminus \{3eb68$

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

HKCU\software\microsoft\windows\currentversion\explorer

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus session in fo \setminus 1$ Opens key:

Opens key:

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

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

folders

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

Opens key:

b2f1-4857-a4ce-a8e7c6ea7d27}

Opens kev:

b2f1-4857-a4ce-a8e7c6ea7d27}\propertybag

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ adb 62392 bc 0711707 e58e70186 cc4 ac2. exemple \ descriptions \ adb 62392 bc 0711707 e58e70186 cc4 ac2. exemple \ descriptions \ adb 62392 bc 0711707 e58e70186 cc4 ac2. exemple \ descriptions \ adb 62392 bc 0711707 e58e70186 cc4 ac2. exemple \ descriptions \ adb 62392 bc 0711707 e58e70186 cc4 ac2. exemple \ descriptions \ adb 62392 bc 0711707 e58e70186 cc4 ac2. exemple \ descriptions \ adb 62392 bc 0711707 e58e70186 cc4 ac2. exemple \ descriptions \ adb 62392 bc 0711707 e58e70186 cc4 ac2. exemple \ descriptions \ adb 62392 bc 0711707 e58e70186 cc4 ac2. exemple \ descriptions \ adb 62392 bc 0711707 e58e70186 cc4 ac2. exemple \ descriptions \ adb 62392 bc 0711707 e58e70186 cc4 ac2. exemple \ descriptions \ adb 62392 bc 0711707 e58e70186 cc4 ac2. exemple \ descriptions \ adb 62392 bc 0711707 e58e70186 cc4 ac2. exemple \ descriptions \ adb 62392 bc 0711707 e58e70186 cc4 ac2. exemple \ adb 62392 bc 0711707 e58e70186 cc4 ac2$

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

 $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ policies\+ explorer$ Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer

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

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

Opens key: $\label{thm:local_hammon} \mbox{HKCU\software\mbox{\sc urrentversion\directmanipulation}} \label{thm:local_hammon}$

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

Opens key: HKCU\software\classes\

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

08002b30309d}\shellfolder

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

08002b30309d}\shellfolder

Opens key: $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus (20d04fe0-the following of the follow$

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

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ clsid \ \{20d04fe0-3aea-1069-1046fe0-3aea-1046fe0$

a2d8-08002b30309d}\shellfolder

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

Opens key:

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

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

08002b30309d}\inprocserver32

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}

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

409d6c4515e9} Opens key:

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

Opens kev: HKLM\software\microsoft\windows\currentversion\explorer\kindmap

Opens key: HKCU\software\classes\.exe

Opens key: HKCR\.exe

HKLM\software\microsoft\com3 Opens key:

Opens key: HKLM\software\microsoft\windowsruntime\clsid

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}

Opens key: HKCR\activatableclasses\clsid

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

b8dc300d9f9d}

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

b8dc300d9f9d}\treatas

Opens key: $HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treat as$ Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{1f486a52 - 3cb1 - 48fd - 8f50 - 48fd - 8f50$

b8dc300d9f9d}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\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

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

b8dc300d9f9d}\inprochandler

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

b8dc300d9f9d}\inprochandler

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

HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-Opens key:

97a27216f98a}\inprocserver32

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

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

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\classes\exefile

Opens key: HKCR\exefile

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

HKCR\exefile\curver Opens key: Opens key: HKCR\exefile\

 $\label{thm:hammon} \mbox{HKCU\software\classes\exefile\shellex\liconhandler} \label{thm:hcu}$ Opens key:

Opens key: HKCR\exefile\shellex\iconhandler

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

Opens key: HKCR\systemfileassociations\.exe

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

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

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

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

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

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 key:

db2c-424c-b029-7fe99a87c641}

Opens key:

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

 $HKCR \setminus wow 6432 \\ node \\ \clsid \\ \cl$ Opens key:

a6bb2164fbd0}\inprocserver32

Opens key:

b587-4786-b4ef-bd1dc332aeae}

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-16b4ea5$ b587-4786-b4ef-bd1dc332aeae}\propertybag

0e22-4760-9afe-ea3317b67173}

Opens key:

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

Opens key:

HKLM\software\wow6432node\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001

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

1923240461-1905901954-2556564120-1001

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directorv

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

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

Opens key: HKCR\folder

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

Opens key: HKCR\folder\shellex\iconhandler

Opens kev: HKCU\software\classes\allfilesystemobjects

Opens key: HKCR\allfilesystemobjects

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

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

Opens key: ${\tt HKCR \backslash directory \backslash docobject}$

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

Opens key: HKCR\folder\docobject

```
Opens key:
                                                          HKCU\software\classes\allfilesystemobjects\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 kev:
                                                         HKCR\folder\clsid
    Opens key:
                                                          HKCU\software\classes\allfilesystemobjects\clsid
    Opens key:
                                                          HKCR\allfilesystemobjects\clsid
    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
                                                         HKCR\wow6432node\clsid\{1649d1cf-deaf-4a68-abe8-
    Opens key:
5c9f68572fd1}\inprocserver32
    Opens key:
                                                         HKCR\exefile\shell\open\
    Opens key:
                                                         HKLM\software\wow6432node\policies\microsoft\windows\explorer
    Opens key:
                                                         HKLM\software\policies\microsoft\windows\explorer
    Opens key:
                                                          \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ explorer
    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 \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{76765b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-3f95-4af2-ac9d-1464b11-364b11-364b11-364b11-364b11-364b11-364b11-364b11-364b11-364b11-364b11-364b11-364b11-364b11-364b11-364b11-364b11-364b11-364b11-364b11-364b11-364b11-364b11-364b11-364b11-364b11-364b11-36
ea55d8994f1a}
    Opens key:
                                                         HKCR\activatableclasses\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}
    Opens key:
                                                         HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}
    Opens key:
                                                         HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}
    Opens key:
                                                          HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\treatas
                                                          HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\
    Opens key:
    Opens key:
                                                         ea55d8994f1a}\inprocserver32
    Opens kev:
                                                         HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprocserver32
    Opens key:
                                                         HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprochandler32
                                                         HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-
    Opens key:
ea55d8994f1a}\inprochandler32
    Opens key:
                                                         HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{76765b11-3f95-4af2-ac9d-46432 \\ node \setminus clsid \setminus \{76765b11-3f95-4af2-ac9d-46442 \\ node \setminus clsid 
ea55d8994f1a}\inprochandler
    Opens key:
                                                         HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprochandler
    Opens kev:
                                                         HKLM\software\microsoft\windowsruntime\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}
                                                          HKCR\activatableclasses\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
    Opens key:
    Opens key:
                                                         HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}
                                                          HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
    Opens key:
    Opens key:
                                                          HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\treatas
    Opens key:
                                                         HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treat as
    Opens key:
                                                         HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32
                                                         HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
    Opens key:
00c04fb6bfc4}\inprocserver32
                                                         HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
    Opens key:
00c04fb6bfc4}\inprochandler32
    Opens key:
                                                         HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler32
                                                         HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
    Opens key:
00c04fb6bfc4}\inprochandler
   Opens key:
                                                         HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler
    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:
                                                         \label{lem:hklmsoftware policies microsoft internet explorer main feature control} \\
    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 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature ignore policies zonemap if esc enabled kb918915 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 Opens kev: settings\zonemap\domains\ Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains HKCU\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\zonemap\domains\ Opens key: HKLM\zonemap\ranges\ Opens key: HKCU\zonemap\ranges\ Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001 Opens key: HKLM\software\wow6432node\microsoft\internet 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 kev: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet$ Opens key: settings\zonemap\ Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap\ Opens key: $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ settings\zonemap\ranges\ Opens kev: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\protocoldefaults\ Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\domains\ HKLM\software\wow6432node\microsoft\windows\currentversion\internet Opens key: settings\zonemap\domains\ Opens key: HKCU\software\microsoft\internet 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 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562 HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562 Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer Opens key: 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 Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc Opens key: HKLM\software\policies\microsoft\windows nt\rpc 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 $\label{lem:hkcu} \mbox{HKCU\software\mbox{\sc urrentversion\internet settings\sc varies} \mbox{\sc urrentversion\sc urrentversion\sc varies} \mbox{\sc urrentversion\sc u$ Opens key: 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 key: $\label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ settings\zones\ Opens key:

Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\0

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\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\1
                        HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\1
 Opens key:
                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
                        HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\zonemap\
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\2
 Opens kev:
                        HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
                        HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\2
 Opens kev:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\3
                        HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\3
 Opens key:
                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
 Opens key:
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 kev:
settings\zones\4
                        HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_localmachine_lockdown
                        HKLM\software\wow6432node\microsoft\internet
 Opens key:
\verb|explorer\main\featurecontrol\feature_localmachine_lockdown|
 Opens key:
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\
 Opens key:
                        HKCU\software\microsoft\windows\currentversion\internet
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 key:
settings\lockdown zones\0
 Opens key:
                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                        HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\1
 Opens key:
settings\lockdown_zones\1
                        \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
 Opens key:
settings\lockdown_zones\1
 Opens key:
                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                        HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\2
 Opens key:
settings\lockdown_zones\2
                        HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
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
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
 Opens key:
                        HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                        HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\3
 Opens key:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
 Opens key:
```

settings\lockdown_zones\4

HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\lockdown_zones\4 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\lockdown zones\4 Opens key: HKCU\software\microsoft\internet 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: 33be-4251-ba85-6007caedcf9d} Opens kev: $HKLM \label{lem:hklm} Which was the simple of the second of the second$ 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 kev: settings\zones\0 Opens key: HKLM\software\microsoft\sqmclient\windows\disabledprocesses\ Opens key: HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8 Opens key: HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows Opens key: HKLM\software\microsoft\telemetryclient\throttlestore\sqm Opens key: HKLM\software\microsoft\telemetryclient\throttlestore Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8 Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sqm Opens key: Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8\13238528 Opens kev: HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8\13238784 Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8\13238784 Opens key: HKCU\software\classes\exefile\progid Opens kev: HKCR\exefile\progid Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ progids \ exefile$ Opens key: HKCU\software\classes\exefile\shell\open\ddeexec Opens key: HKCR\exefile\shell\open\ddeexec $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\app\ paths\schtasks.exe}} \\$ Opens key: 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: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \mbox{microsoft \windows \current version \explorer \mbox{mountpoints 2$ \cpc \volume} \end{tabular} \label{lem:hkcu}$ 11e3-be65-806e6f6e6963}\ Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\setup Opens key: HKLM\software\microsoft\windows\currentversion\setup Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion Opens key: $HKLM \setminus system \setminus current control \setminus device classes \setminus \{53f5630d-b6bf-11d0-b6b$ 94f2-00a0c91efb8b} Opens kev: $HKLM \ system \ current control \ device classes \ \ \{53f5630d-b6bf-11d0-b$ 94f2-00a0c91efb8b}\properties Opens key: $\label{prop:hkcu} HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \coloner \dashed \current \current \dashed \current \current \dashed \current \current \current \dashed \current \current$ 11e3-be65-806e6f6e6963}\ 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\system\currentcontrolset\control\session manager\appcompatibility Opens key: HKLM\software\wow6432node\policies\microsoft\windows\appcompat

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

Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers HKLM\software\wow6432node\microsoft\windows

Opens key:

nt\currentversion\appcompatflags

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

nt\currentversion\appcompatflags\custom\schtasks.exe

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \end{tabular} in \begin{tabular}{ll} Software \end{tabu$ Opens key:

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

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

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

Opens key: HKCR\applications\schtasks.exe

Opens key: HKCU\software\microsoft\windows\shell\associations

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

options\conhost.exe

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

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\console\truetypefont Opens key: HKLM\software\microsoft\windows nt\currentversion\console\fullscreen

Opens key: HKCU\console Opens key: HKCU\console\

Opens key: HKCU\console\%systemroot%_syswow64_schtasks.exe
Opens key: HKCU\console\%systemroot%\syswow64\schtasks.exe
Opens key: HKLM\system\currentcontrol\set\control\nls\locale

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

Opens key: HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange

Opens key: HKLM\software\microsoft\ctf\compatibility\conhost.exe
Opens key: HKLM\software\microsoft\windows\windows error reporting\wmr

Opens key:

HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\system\currentcontrolset\control\sqmservicelist

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

Opens key: HKCR\appid\schtasks.exe

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{0f87369f-a4e5-4cfc-bd3e-

73e6154572dd}

Opens key: $\begin{tabular}{ll} HKCR\activatableclasses\c]sid\end{tabular} \begin{tabular}{ll} HKCR\activatableclasses\c]sid\end{tabular} \begin{tabular}{ll} HKCU\software\c]asses\wow6432node\c]sid\end{tabular} \begin{tabular}{ll} HKCU\software\c]asses\wow6432node\c]sid\end{tabular} \begin{tabular}{ll} HKCU\software\c]asses\wow6432node\c]sid\end{tabular} \begin{tabular}{ll} HKCU\software\c]asses\wow6432node\c]asses\c$

73e6154572dd}

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

73e6154572dd}\treatas

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

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\currentcontrol\etailanguages\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:

 $HKLM \label{lem:hklm} White the latest of the latest of$

 $\label{thm:current} Queries \ value: \\ HKLM\system\currentcontrolset\control\nls\sorting\versions[]$

Queries value: HKCU\software\microsoft\windows

 $\verb|nt\currentversion\appcompatflags[showdebuginfo]| \\$

Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[adb62392bc0711707e58e70186cc4ac2] Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\windows[loadappinit_dlls]

 $\label{thm:linear} Queries \ value: \\ HKLM\system\current control set\control\spans{fipsalgorithm} it is not control\spans{fipsalgorithm} for all the properties of the prop$

Queries value: HKLM\system\currentcontrol\sa[fipsalgorithmpolicy]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]

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

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

Oueries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\calebox{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\cite{2.000} [parsing name]$

Queries value

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

Queries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ Ficon 1$

Queries value:

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

Oueries value

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

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: HKLM\system\currentcontrol\set\control\nls\sorting\versions[000602xx]
Queries value: HKLM\system\currentcontrol\set\control\nls\sorting\ids[en-us]
Queries value: HKLM\system\currentcontrol\set\control\nls\sorting\ids[en]

Oueries value:

 $\label{thm:local-continuous} HKLM \software \wow6432 node \mbox{$d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27} \ [category]$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

```
b2f1-4857-a4ce-a8e7c6ea7d27}[relativepath]
    Queries value:
HKLM \setminus software \setminus wow6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{d65231b0-d1011, d1011, d101
b2f1-4857-a4ce-a8e7c6ea7d27}[parsingname]
    Oueries value:
HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{d65231b0-d1014, d1014, d10
b2f1-4857-a4ce-a8e7c6ea7d27}[infotip]
    Oueries value:
b2f1-4857-a4ce-a8e7c6ea7d27}[localizedname]
    Oueries value:
b2f1-4857-a4ce-a8e7c6ea7d27}[icon]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}[security]
    Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ folds \ defect \ folds \ 
b2f1-4857-a4ce-a8e7c6ea7d27}[streamresource]
    Oueries value:
b2f1-4857-a4ce-a8e7c6ea7d27}[streamresourcetype]
    Queries value:
b2f1-4857-a4ce-a8e7c6ea7d27}[localredirectonly]
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}[roamable]
    Queries value:
b2f1-4857-a4ce-a8e7c6ea7d27}[precreate]
    Oueries value:
b2f1-4857-a4ce-a8e7c6ea7d27}[stream]
    Oueries value:
b2f1-4857-a4ce-a8e7c6ea7d27}[publishexpandedpath]
b2f1-4857-a4ce-a8e7c6ea7d27}[attributes]
    Queries value:
b2f1-4857-a4ce-a8e7c6ea7d27}[foldertypeid]
    Oueries value:
b2f1-4857-a4ce-a8e7c6ea7d27}[initfolderhandler]
                                                                    HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps]
    Queries value:
    Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ (explorer[maximizeapps]) \ and \ (explorer[maximizeapps]
HKLM\software\microsoft\windows\currentversion\policies\explorer[enableshellexecutehooks]
                                                                    HKLM\software\microsoft\sqmclient\windows[ceipenable]
    Queries value:
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
                                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
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[foldervalueflags]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}1
    Oueries value:
                                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32[]
    Queries value:
                                                                    HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
```

409d6c4515e9}[drivemask]

Queries value:

```
HKLM\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]
 Oueries value:
                       HKLM\software\microsoft\windows\currentversion\explorer\kindmap[.exe]
 Queries value:
                       HKCR\.exe[content type]
 Queries value:
                       HKLM\software\microsoft\com3[com+enabled]
                       HKCR \ wow 6432 node \ clsid \ \{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\}[]
 Queries value:
 Queries value:
                       HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[inprocserver32]
                       HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
 Queries value:
b8dc300d9f9d}\inprocserver32[]
                       HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
 Queries value:
b8dc300d9f9d}\inprocserver32[threadingmodel]
 Oueries value:
                       HKLM\software\microsoft\ole[maxsxshashcount]
 Queries value:
                       HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
 Queries value:
                       HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-
97a27216f98a}\inprocserver32[]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
 Oueries value:
                       HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
                       HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
 Oueries value:
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
 Queries value:
                       HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
 Oueries value:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \current version \explorer \advanced [show superhidden] \end{tabular}
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
 Queries 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]
 Queries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced [show type overlay]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showstatusbar]
                       HKCR\.exe[]
 Queries value:
                       HKCR\exefile[docobject]
 Oueries value:
                       HKCR\systemfileassociations\.exe[docobject]
 Queries value:
 Queries value:
                        HKCR\exefile[browseinplace]
 Queries value:
                       HKCR\systemfileassociations\.exe[browseinplace]
                       HKCR\exefile[isshortcut]
 Queries value:
                       HKCR\systemfileassociations\.exe[isshortcut]
 Oueries value:
 Queries value:
                       HKCR\exefile[alwaysshowext]
 Queries value:
                       HKCR\systemfileassociations\.exe[alwaysshowext]
 Queries value:
                       HKCR\exefile[nevershowext]
 Oueries value:
                       HKCR\systemfileassociations\.exe[nevershowext]
 Oueries value:
db2c-424c-b029-7fe99a87c641}[category]
 Queries value:
db2c-424c-b029-7fe99a87c641}[name]
db2c-424c-b029-7fe99a87c641}[parentfolder]
 Queries value:
db2c-424c-b029-7fe99a87c641}[description]
 Queries value:
```

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

Queries value:

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

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma(b4bfcc3a-db2c-424c-b029-7fe99a87c641)\[localized name]$

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

 $\label{thm:local-state} $HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}[streamresourcetype]}$

Queries value:

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

Queries value

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

Queries value:

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

Queries value:

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

Oueries value:

 $\label{thm:local-soft-windows} HKLM\software\wow6432 node\microsoft\windows\current version\explorer\folder descriptions\gamma\gam$

Oueries value:

Queries value:

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

Oueries value:

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

folders[desktop]

Queries value: HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-

a6bb2164fbd0}\inprocserver32[]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value

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

Queries value:

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

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dcb587-4786-b4ef-bd1dc332aeae}[parsingname]

Queries value:

Queries value:

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

Queries value:

Queries value:

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value

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

Queries value:

Oueries value:

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

Oueries value:

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

Queries value

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

Oueries value:

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

Oueries value:

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

 $\label{thm:condition} Queries \ value: \\ HKCU \ software \ \ microsoft \ \ windows \ \ current version \ \ explorer \ \ shell$

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsingname]

Oueries value

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

Oueries value:

 $\label{thm:local-prop} $HKLM \setminus software \setminus wow 6432 node \\ icrosoft \setminus windows \setminus explorer \setminus folder descriptions \setminus \{5e6c858f-0e22-4760-9afe-ea3317b67173\}[localized name]$

Oueries value:

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

Queries value:

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

Queries value

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

Queries value:

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

Oueries value:

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

Queries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[roamable]

Queries value:

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

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1}{2} e6c858f-0e22-4760-9 af e-ea3317 b67173 \footnote{1}{2} [stream]$

Queries value:

```
0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
  Queries value:
HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{5e6c858f-4c41\} \\ for the first of the first o
0e22-4760-9afe-ea3317b67173}[attributes]
0e22-4760-9afe-ea3317b67173}[foldertypeid]
  Oueries value:
0e22-4760-9afe-ea3317b67173}[initfolderhandler]
                                    Oueries value:
1923240461-1905901954-2556564120-1001[profileimagepath]
  Oueries value:
                                    HKCR\directory[docobject]
  Queries value:
                                    HKCR\folder[docobject]
                                    HKCR\allfilesystemobjects[docobject]
  Oueries value:
  Queries value:
                                    HKCR\directory[browseinplace]
  Queries value:
                                    HKCR\folder[browseinplace]
                                    HKCR\allfilesystemobjects[browseinplace]
  Oueries value:
  Queries value:
                                    HKCR\directory[isshortcut]
  Oueries value:
                                    HKCR\folder[isshortcut]
  Queries value:
                                    HKCR\allfilesystemobjects[isshortcut]
  Queries value:
                                    HKCR\directory[alwaysshowext]
  Queries value:
                                    HKCR\directory[nevershowext]
  Oueries value:
                                    HKCR\folder[nevershowext]
  Oueries value:
                                    HKCR\allfilesvstemobjects[nevershowext]
  Queries value:
                                    HKCR\exefile[nostaticdefaultverb]
                                    HKCR\exefile\shell[]
  Oueries value:
  Queries value:
                                    HKCR\exefile\shell\open[neverdefault]
  Queries value:
                                    HKCR\wow6432node\clsid\{1649d1cf-deaf-4a68-abe8-
5c9f68572fd1}\inprocserver32[]
                                    HKCR\exefile\shell\open\command[delegateexecute]
  Queries value:
                                    HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}[]
  Oueries value:
  Queries value:
                                    HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprocserver32[inprocserver32]
  Queries value:
                                    HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprocserver32[]
  Queries value:
                                    HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprocserver32[threadingmodel]
  Oueries value:
                                    HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[]
  Queries value:
                                    HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[inprocserver32]
                                    HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
  Queries value:
00c04fb6bfc4}\inprocserver32[]
                                    HKCR\wow6432 node\clsid\{7b8a2d94-0ac9-11d1-896c-1}
  Oueries value:
00c04fb6bfc4}\inprocserver32[threadingmodel]
                                    HKLM\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings[security_hklm_only]
  Queries value:
                                    HKLM\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
                                    HKCU\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings[createuricachesize]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Queries value:
                                    HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Oueries value:
                                    HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
                                    HKCU\software\policies\microsoft\windows\currentversion\internet
  Oueries value:
settings[enablepunycode]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[enablepunycode]
                                    HKLM\software\policies\microsoft\internet
  Queries value:
explorer\security[disablesecuritysettingscheck]
  Queries value:
                                    HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
                                    HKLM\system\setup[oobeinprogress]
  Oueries value:
                                    HKLM\system\setup[systemsetupinprogress]
  Oueries value:
  Queries value:
                                    HKLM\software\microsoft\rpc[idletimerwindow]
  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]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
```

settings\zones\4[flags]
 Oueries value: HKCU\software\microsoft\internet

```
explorer\main\featurecontrol\feature_localmachine_lockdown[adb62392bc0711707e58e70186cc4ac2.exe]
Oueries value:
             HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
             HKLM\software\wow6432node\microsoft\internet
Queries value:
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]
             HKCU\software\policies\microsoft\windows\currentversion\internet
Queries value:
settings[specialfolderscachesize]
             HKCU\software\microsoft\windows\currentversion\internet
Oueries value:
settings[specialfolderscachesize]
Queries value:
             HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
Oueries value:
33be-4251-ba85-6007caedcf9d}[category]
Oueries value:
33be-4251-ba85-6007caedcf9d}[name]
Queries value:
33be-4251-ba85-6007caedcf9d}[parentfolder]
Oueries value:
33be-4251-ba85-6007caedcf9d}[description]
Oueries value:
33be-4251-ba85-6007caedcf9d}[relativepath]
Queries value:
33be-4251-ba85-6007caedcf9d}[parsingname]
Queries value:
33be-4251-ba85-6007caedcf9d}[infotip]
Queries value:
33be-4251-ba85-6007caedcf9d}[localizedname]
Oueries value:
33be-4251-ba85-6007caedcf9d}[icon]
Queries value:
33be-4251-ba85-6007caedcf9d}[security]
Queries value:
33be-4251-ba85-6007caedcf9d}[streamresource]
Queries value:
33be-4251-ba85-6007caedcf9d}[streamresourcetype]
Oueries value:
33be-4251-ba85-6007caedcf9d}[localredirectonly]
Queries value:
-HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8
33be-4251-ba85-6007caedcf9d}[roamable]
Queries value:
33be-4251-ba85-6007caedcf9d}[precreate]
33be-4251-ba85-6007caedcf9d}[stream]
Oueries value:
33be-4251-ba85-6007caedcf9d}[publishexpandedpath]
Oueries value:
33be-4251-ba85-6007caedcf9d}[attributes]
Queries value:
33be-4251-ba85-6007caedcf9d}[foldertypeid]
Queries value:
33be-4251-ba85-6007caedcf9d}[initfolderhandler]
             HKCU\software\microsoft\windows\currentversion\explorer\user shell
Oueries value:
folders[cache]
Queries value:
c0e9-4171-908e-08a611b84ff6}[category]
Queries value:
```

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

Queries value:

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

Oueries value

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

Oueries value:

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

Oueries value:

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

Queries value

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot\{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[streamresource]$

Queries value:

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

Queries value:

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

Oueries value:

 $\label{limits} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fold$

Oueries value:

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

Queries value:

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

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}[publishexpandedpath]$

Queries value:

 $\label{local-ham} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\$

Queries value:

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

Oueries value:

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

Oueries 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]

 $\label{thm:linear} Queries \ value: \\ HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet \\ \\$

settings\zones\0[1806]

Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[e00556a0]

 $Queries \ value: \\ HKLM\software\microsoft\sqmclient\windows[studyid]$

 $\label{thm:linear} Queries \ value: \\ HKLM \ software \ microsoft \ telemetry client \ sample store \ sqm[sample dout] \\$

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

Queries value:

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

Oueries 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:

 $\label{thm:constraint} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \{d5291c64-7c88-1c44-$

```
11e3-be65-806e6f6e6963}[data]
   Oueries value:
11e3-be65-806e6f6e6963}[generation]
   Queries value:
                                                     HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
   Queries value:
                                                     HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
   Oueries value:
11e3-be65-806e6f6e6963}[data]
   Queries value:
HKCU \setminus software \setminus icrosoft \setminus indows \setminus current version \setminus explorer \setminus mountpoints 2 \setminus cpc \setminus volume \setminus \{d5291c63-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus cpc \setminus volume \setminus \{d5291c63-five a content version \setminus cpc \setminus 
11e3-be65-806e6f6e6963}[generation]
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
   Queries value:
                                                     HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
   Queries value:
                                                     HKCU\software\microsoft\windows\shell\associations[showtoast]
   Queries value:
                                                     HKLM\system\currentcontrolset\control\session
manager[pendingfilerenameoperations2]
                                                     HKLM\system\currentcontrolset\control\session
   Oueries value:
manager[pendingfilerenameoperations]
   Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
   Queries value:
                                                     HKLM\software\microsoft\windows
nt\currentversion\compatibility32[conhost]
                                                     HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\windows[loadappinit_dlls]
   Oueries value:
                                                     HKCU\console[screencolors]
   Queries value:
                                                     HKCU\console[popupcolors]
   Queries value:
                                                     HKCU\console[insertmode]
   Oueries value:
                                                     HKCU\console[quickedit]
   Queries value:
                                                     HKCU\console[codepage]
   Oueries value:
                                                     HKCU\console[screenbuffersize]
   Queries value:
                                                     HKCU\console[windowsize]
   Queries value:
                                                     HKCU\console[windowposition]
   Oueries value:
                                                     HKCU\console[fontsize]
   Queries value:
                                                     HKCU\console[fontfamily]
   Oueries value:
                                                     HKCU\console[fontweight]
   Queries value:
                                                     HKCU\console[facename]
   Oueries value:
                                                     HKCU\console[cursorsize]
   Queries value:
                                                     HKCU\console[historybuffersize]
   Queries value:
                                                     HKCU\console[numberofhistorybuffers]
   Oueries value:
                                                     HKCU\console[historynodup]
                                                     HKCU\console[colortable00]
   Oueries value:
   Oueries value:
                                                     HKCU\console[colortable01]
   Queries value:
                                                     HKCU\console[colortable02]
   Queries value:
                                                     HKCU\console[colortable03]
   Queries value:
                                                     HKCU\console[colortable04]
   Oueries value:
                                                     HKCU\console[colortable05]
                                                     HKCU\console[colortable061
   Oueries value:
   Queries value:
                                                     HKCU\console[colortable07]
   Oueries value:
                                                     HKCU\console[colortable081
   Queries value:
                                                     HKCU\console[colortable09]
   Queries value:
                                                     HKCU\console[colortable10]
   Oueries value:
                                                     HKCU\console[colortable11]
   Queries value:
                                                     HKCU\console[colortable12]
   Oueries value:
                                                     HKCU\console[colortable131
   Queries value:
                                                     HKCU\console[colortable14]
   Queries value:
                                                     HKCU\console[colortable15]
   Oueries value:
                                                     HKCU\console[loadconime]
   Queries value:
                                                     HKCU\console[extendededitkey]
   Oueries value:
                                                     HKCU\console[extendededitkeycustom]
                                                     HKCU\console[worddelimiters]
   Queries value:
   Oueries value:
                                                     HKCU\console[trimleadingzeros]
   Queries value:
                                                     HKCU\console[enablecolorselection]
   Queries value:
                                                     HKCU\console[scrollscale]
   Queries value:
                                                     HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
                                                     HKLM\system\currentcontrolset\control\nls\locale[00000409]
   Oueries value:
   Queries value:
                                                     HKLM\system\currentcontrolset\control\nls\language groups[1]
   Queries value:
                                                     HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange[1252]
   Queries value:
                                                     HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
                                                     HKLM\software\wow6432node\microsoft\windows
   Queries value:
nt\currentversion\compatibilitv32[schtasks]
```

HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]

 $\label{local-hkkk} HKLM \system \current control set \control \sa[every one includes an ony mous] \\ HKCR \system \cklimetries \system \syste$

Queries value: $HKCR\wow6432$ node\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprocserver32[inprocserver32]

Oueries value:

Queries value:

Queries value: Queries value: 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]