Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 246, Task ID: 982

Task ID: 982

Risk Level: 7

Date Processed: 2016-04-28 13:14:19 (UTC)

Processing Time: 2.64 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\280c53057f49089a8bbef69fce3e81cd.exe"

Sample ID: 246 Type: basic Owner: admin

Label: 280c53057f49089a8bbef69fce3e81cd

Date Added: 2016-04-28 12:45:15 (UTC)

File Type: PE32:win32:gui File Size: 376040 bytes

MD5: 280c53057f49089a8bbef69fce3e81cd

SHA256: dcf31db18983784dcecab6c4557722cb32cc384121b5b4cc77930b071f747c25

Description: None

Pattern Matching Results

7 Signed by adware producer [Adware, PUA]

2 PE: Nonstandard section

4 Packer: NSIS [Nullsoft Scriptable Install System]

Static Events

Anomaly: PE: Contains a virtual section

Anomaly: PE: Contains one or more non-standard sections

Process/Thread Events

Creates process: C:\windows\temp\280c53057f49089a8bbef69fce3e81cd.exe

["C:\windows\temp\280c53057f49089a8bbef69fce3e81cd.exe"]

Terminates process: C:\Windows\Temp\280c53057f49089a8bbef69fce3e81cd.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Creates: C:\Users\Admin\AppData\Local\Temp\

Creates: C:\Users\Admin\AppData\Local\Temp\nslB06F.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\nsaB0CD.tmp

Creates: C:\Users
Creates: C:\Users\Admin
Creates: C:\Users\Admin\AppData
Creates: C:\Users\Admin\AppData\Local
Creates: C:\Users\Admin\AppData\Local\Temp

Creates: C:\Users\Admin\AppData\Local\Temp\nsaBOCD.tmp\tkDecript.dll
Creates: C:\Users\Admin\AppData\Local\Temp\nsaBOCD.tmp\version.dll
Opens: C:\Windows\Prefetch\280C53057F49089A8BBEF69FCE3E8-6305A30E.pf

Opens: C:\Windows

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

Opens: C:\Windows\SysWOW64

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

Opens: C:\Windows\Temp\280c53057f49089a8bbef69fce3e81cd.exe

Opens: C:\Windows\SysWOW64\ntdll.dll Opens: C:\Windows\SysWOW64\kernel32.dll Opens: C:\Windows\SysWOW64\KernelBase.dll Opens: C:\Windows\apppatch\sysmain.sdb Opens: C:\Windows\apppatch\AcGenral.dll C:\Windows\apppatch\AcLayers.dll Opens: Opens: C:\Windows\SysWOW64\sechost.dll Opens: C:\Windows\SysWOW64\uxtheme.dll C:\Windows\SysWOW64\winmm.dll Opens: C:\Windows\SysWOW64\samcli.dll Opens: C:\Windows\SysWOW64\msacm32.dll Opens: Opens: C:\Windows\SysWOW64\version.dll

 Opens:
 C:\Windows\SysWOW64\msacm32.dll

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

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

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

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

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

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

Opens: C:\Windows\SysWOW64\profapi.dll
Opens: C:\Windows\SysWOW64\SHCore.dll

```
C:\Windows\SysWOW64\sfc.dll
   Opens:
                                              C:\Windows\SysWOW64\sfc_os.dll
   Opens:
                                              C:\windows\temp\280c53057f49089a8bbef69fce3e81cd.exe.Manifest
   Opens:
   Opens:
                                              C:\Windows\SysWOW64\msvcrt.dll
                                              C:\Windows\SysWOW64\bcryptprimitives.dll
   Opens:
   Opens:
                                              C:\Windows\SysWOW64\cryptbase.dll
                                              C:\Windows\SysWOW64\sspicli.dll
   Opens:
   Opens:
                                               C:\Windows\SysWOW64\rpcrt4.dll
   Opens:
                                              C:\Windows\SysWOW64\gdi32.dll
                                              C:\Windows\SysWOW64\user32.dll
   Opens:
                                              C:\Windows\SysWOW64\shlwapi.dll
   Opens:
   Opens:
                                              C:\Windows\SysWOW64\ole32.dll
   Opens:
                                               C:\Windows\SysWOW64\oleaut32.dll
   Opens:
                                               C:\Windows\SysWOW64\advapi32.dll
   Opens:
                                              C:\Windows\SysWOW64\shell32.dll
   Opens:
                                              C:\Windows\SysWOW64\iertutil.dll
                                              C:\Windows\SysWOW64\wininet.dll
   Opens:
                                               C:\Windows\SysWOW64\urlmon.dll
   Opens:
                                              C:\Windows\SysWOW64\cfgmgr32.dll
   Opens:
   Opens:
                                              C:\Windows\SysWOW64\devobj.dll
   Opens:
                                              C:\Windows\SysWOW64\setupapi.dll
   Opens:
                                              C:\Windows\SysWOW64\imm32.dll
   Opens:
                                              C:\Windows\SysWOW64\msctf.dll
                                              C:\Windows\WinSxS\x86_microsoft.windows.common-
   Opens:
controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954
                                               C:\Windows\WinSxS\x86_microsoft.windows.common-
   Opens:
controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954\comctl32.dll
   Opens:
                                              C:\Windows\SysWOW64\shfolder.dll
   Opens:
                                              C:\Windows\Globalization\Sorting\SortDefault.nls
   Opens:
                                              C:\
   Opens:
                                              C:\Windows\SysWOW64\clbcatq.dll
   Opens:
                                              C:\Windows\SysWOW64\propsys.dll
                                              Opens:
4C77-AF34-C647E37CA0D9}.1.ver0x00000000000000e.db
   Opens:
                                              C:\Windows\SysWOW64\desktop.ini
   Opens:
                                              C:\Users\Admin\Desktop\desktop.ini
   Opens:
                                              C:\Users
   Opens:
                                              C:\Users\Admin
   Opens:
                                              C:\Users\Admin\AppData
   Opens:
                                              C:\Users\Admin\AppData\Local
   Opens:
                                              C:\Users\Admin\AppData\Local\Temp
   Opens:
                                               C:\Users\Admin\AppData\Local\Temp\nslB06F.tmp
                                              C:\Users\Admin\AppData\Local\Temp\nsaBOCD.tmp
   Opens:
   Opens:
                                              C:\Users\Admin\AppData\Local\Temp\nsaBOCD.tmp\tkDecript.dll
                                              {\tt C:\Users\Admin\AppData\Local\Temp\nsaBOCD.tmp\version.dll}\\
   Opens:
   Writes to:
                                              \verb|C:\Users\Admin\AppData\Local\Temp\nsaBOCD.tmp\tkDecript.dll|\\
   Writes to:
                                              C:\Users\Admin\AppData\Local\Temp\nsaBOCD.tmp\version.dll
   Reads from:
                                              C:\Users\Admin\Desktop\desktop.ini
   Reads from:
                                               C:\Windows\Temp\280c53057f49089a8bbef69fce3e81cd.exe
   Deletes:
                                              C: \verb|\draw| AppData \verb|\draw| Imp \verb|\draw| Signature | Signature 
   Deletes:
                                              C:\Users\Admin\AppData\Local\Temp\nsaBOCD.tmp
   Deletes:
                                              C:\Users\Admin\AppData\Local\Temp\nsaBOCD.tmp\tkDecript.dll
```

Deletes: C:\Users\Admin\AppData\Local\Temp\nsaBOCD.tmp\version.dll

Opens key:

Opens key:

Opens key:

Windows Registry Events	
Opens key:	HKLM\software\microsoft\wow64
Opens key:	<pre>HKLM\system\currentcontrolset\control\safeboot\option</pre>
Opens key:	<pre>HKLM\system\currentcontrolset\control\srp\gp\dll</pre>
Opens key:	
HKLM\software\wow6	5432node\policies\microsoft\windows\safer\codeidentifiers
Opens key:	<pre>HKLM\software\policies\microsoft\windows\safer\codeidentifiers</pre>
Opens key:	<pre>HKCU\software\policies\microsoft\windows\safer\codeidentifiers</pre>
Opens key:	<pre>HKLM\system\currentcontrolset\control\nls\customlocale</pre>
Opens key:	<pre>HKLM\system\currentcontrolset\control\nls\language</pre>
Opens key:	<pre>HKLM\system\currentcontrolset\control\mui\uilanguages</pre>
Opens key:	<pre>HKLM\system\currentcontrolset\control\mui\uilanguages\en-us</pre>
Opens key:	<pre>HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete</pre>
Opens key:	<pre>HKLM\software\wow6432node\policies\microsoft\mui\settings</pre>
Opens key:	<pre>HKLM\software\policies\microsoft\mui\settings</pre>
Opens key:	HKCU\
Opens key:	$\label{partial} \mbox{HKCU\control panel\desktop\muicached\mbox{\mbox{\backslash}} machine language configuration} \\$
Opens key:	HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
Opens key:	<pre>HKCU\software\policies\microsoft\control panel\desktop</pre>
Opens key:	<pre>HKCU\control panel\desktop\languageconfiguration</pre>
Opens key:	HKCU\control panel\desktop
Opens key:	<pre>HKCU\control panel\desktop\muicached</pre>
Opens key:	HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key:	<pre>HKLM\system\currentcontrolset\control\nls\sorting\versions</pre>

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} in the constant \end{tabular} and \end{tabular} in the constant \end{tabular} and \end{tabular} in the constant \end{tabular} and \end{tabular} in the constant \end{tabular} in the constant \end{tabular} and \end{tabular} in the constant \end{tabular} and \end{tabular} in the constant \end{tabular} and \end{tabular} and \end{tabular} in the constant \end{tabular} and \end{tabular}$

HKCU\software\microsoft\windows nt\currentversion\appcompatflags

 $\label{lem:hklm} \verb+Kklm \+ system \+ current controls et \+ control \+ session \+ manager$

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

protection

Opens key: HKLM\software\policies\microsoft\windows nt\windows file protection

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\disable8and16bitmitigation

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

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

Opens key:

HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\gre_initialize

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

nt\currentversion\compatibility32

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

compatibility

Opens key:

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

Opens key: HKLM\software\policies\microsoft\sqmclient\windows Opens key: HKLM\software\microsoft\sqmclient\windows Opens key: HKLM\software\wow6432node\microsoft\ole Opens key: HKLM\software\wow6432node\microsoft\ole\tracing

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

Opens key:

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

Opens key: HKLM\software\microsoft\windows\currentversion\setup Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side \ assembly storage roots$ HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file Opens key:

execution options

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

options\dllnxoptions

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

Opens key:

 $HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| windows \verb|\currentversion\\| policies \verb|\explorer|| explorer | leading to the context of the$

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

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

Opens key:

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

Opens key: HKCU\software\classes\

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

08002b30309d}\shellfolder

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

08002b30309d}\shellfolder

Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \clsid \closer{lem:hkcu} \end{tabular} $$ -20d04fe0-down \closer{lem:hkcu} \end{tabular} $$ -20$

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

a2d8-08002b30309d}\shellfolder

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

Opens key:

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

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

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

08002b30309d}\inprocserver32

Opens key:

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

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c64-7c88-4cq24, cpc, volume\} \ d5291c64-7c88-4cq24, cpc, volume \ d5291c64-7c88-4cq24, cpc, volume\} \ d5291c64-7c88-4cq24, cpc, volume \ d5291c64-7c88-4cq24, cpc, volume\} \ d5291c64-7c84, cp$

11e3-be65-806e6f6e6963}\

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

Opens key: HKCR\drive\shellex\folderextensions

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

4442-804e-409d6c4515e9}

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

409d6c4515e9}

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

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

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

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

97a27216f98a}\inprocserver32

HKCU\software\classes\directory 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
    Opens key:
                                                               HKCU\software\classes\folder\shellex\iconhandler
    Opens key:
                                                               HKCR\folder\shellex\iconhandler
    Opens key:
                                                               HKCU\software\classes\allfilesystemobjects
    Opens key:
                                                               {\it HKCR} \verb|\| all file system objects
    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
                                                               HKLM \ system \ current control \ device classes \ \ \{53f5630d-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b
    Opens key:
94f2-00a0c91efb8b}
    Opens key:
                                                               HKLM \ system \ current control \ device classes \ \ \{53f5630d-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b
94f2-00a0c91efb8b}\properties
                                                               HKCU\software\classes\folder\docobject
    Opens key:
    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
                                                               HKCR\allfilesystemobjects\browseinplace
    Opens key:
    Opens kev:
                                                               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:
                                                               HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-
a6bb2164fbd0}\inprocserver32
    Opens key:
                                                               HKLM\software\microsoft\com3
    Opens key:
                                                               HKLM\software\microsoft\windowsruntime\clsid
                                                               Opens key:
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
                                                               HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas
    Opens key:
    Opens key:
                                                               HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32
    Opens key:
                                                               HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32
                                                               Opens kev:
b8dc300d9f9d}\inprochandler32
                                                               HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
    Opens key:
b8dc300d9f9d}\inprochandler32
    Opens key:
                                                               b8dc300d9f9d}\inprochandler
    Opens key:
                                                               HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler
    Opens key:
Opens key:
db2c-424c-b029-7fe99a87c641}
db2c-424c-b029-7fe99a87c641}\propertybag
    Opens key:
                                                               HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
    Opens key:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in folders
    Opens key:
                                                               HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
    Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ known foldersettings
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b264, 1b3ea5dc-b264, 1
b587-4786-b4ef-bd1dc332aeae}
    Opens kev:
```

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-

Opens key:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus current \\ version \setminus explorer \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus current \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus current \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus current \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus current \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus current \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus current \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus current \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus current \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus current \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus current \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus current \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus current \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus current \\ descriptions \setminus \{3eb685 \\ db-microsoft \setminus windows \setminus (3eb685 \\ db-microsoft \setminus (3eb6$ 65f9-4cf6-a03a-e3ef65729f3d}\propertybag

0e22-4760-9afe-ea3317b67173}

Opens kev:

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

HKLM\software\wow6432node\microsoft\windows

nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001

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

1923240461-1905901954-2556564120-1001

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c63-7c88-4cq24, cpc, volume\} \ d5291c63-7c88-4cq24, cpc, volume \ d5291c63-7c88-4cq24, cpc, volume\} \ d5291c63-7c88-4cq24, cpc, volume \ d5291c63-7c88-4cq24, cpc, volume\} \ d5291c63-7c84, cp$

11e3-be65-806e6f6e6963}\

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

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

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled] Oueries 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]

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

us[alternatecodepage]

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

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

Queries value:

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

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

HKCU\software\microsoft\windows Queries value:

nt\currentversion\appcompatflags[showdebuginfo]

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

Queries value: HKLM\software\policies\microsoft\windows nt\windows file

protection[knowndlllist]

HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled] Queries value:

 $HKLM \verb|\system| current controlset| control \verb|\lag| fips algorithm policy]$ Oueries value:

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

HKLM\software\wow6432node\microsoft\windows Queries value: nt\currentversion\compatibility32[280c53057f49089a8bbef69fce3e81cd] HKLM\software\wow6432node\microsoft\windows Oueries value:

nt\currentversion\windows[loadappinit_dlls]

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

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

Oueries value: HKLM\software\wow6432node\microsoft\windows\windows error

reporting\wmr[disable]

Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]

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

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

options\dllnxoptions[usefilter]

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

options\dllnxoptions[280c53057f49089a8bbef69fce3e81cd.exe]

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx] Oueries value:

Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us] Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en]

Oueries value:

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

HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value:

08002b30309d}\shellfolder[attributes]

Oueries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder[callforattributes]

Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder[restrictedattributes]

Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder[foldervalueflags]

```
Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{20d04fe0-3aea-1069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8
08002b30309d}]
                                                               HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
08002b30309d}\inprocserver32[]
    Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c64-7c88-4cq24, cpc, volume\} \ d5291c64-7c88-4cq24, cpc, volume \ d5291c64-7c88-4cq24, cpc, volume\} \ d5291c64-7c88-4cq24, cpc, volume \ d5291c64-7c88-4cq24, cpc, volume\} \ d5291c64-7c84, cp
11e3-be65-806e6f6e6963}[data]
    Oueries value:
11e3-be65-806e6f6e6963}[generation]
    Oueries value:
                                                                HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
    Oueries value:
    Queries 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]
                                                               HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
    Oueries value:
    Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
    Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ advanced \ advanced \ advanced \ advanced \ adva
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]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
    Oueries value:
                                                               HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
    Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced [nonetcrawling]
    Queries 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\currentversion\explorer\advanced[showtypeoverlay]
    Queries value:
Oueries value:
                                                               HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-
97a27216f98a}\inprocserver32[]
                                                              HKCR\directory[docobject]
    Oueries value:
    Queries value:
                                                               HKCR\folder[docobject]
    Queries value:
                                                               HKCR\allfilesystemobjects[docobject]
    Queries value:
                                                               HKCR\directory[browseinplace]
    Queries value:
                                                               HKCR\folder[browseinplace]
    Oueries value:
                                                               HKCR\allfilesystemobjects[browseinplace]
                                                               HKCR\directory[isshortcut]
    Queries value:
    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\wow6432node\clsid\{75847177-f077-4171-bd2c-
a6bb2164fbd0}\inprocserver32[]
    Queries value:
                                                               HKLM\software\microsoft\com3[com+enabled]
                                                               HKCR \ wow 6432 node \ clsid \ \{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\}[]
    Queries value:
                                                               Oueries value:
b8dc300d9f9d}\inprocserver32[inprocserver32]
                                                              HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
    Oueries value:
b8dc300d9f9d}\inprocserver32[]
                                                              HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
    Queries value:
b8dc300d9f9d}\inprocserver32[threadingmodel]
    Queries value:
                                                               HKLM\software\microsoft\ole[maxsxshashcount]
```

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\folde$

Queries value:

Queries value:

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

Oueries value:

 $\label{thm:local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \begin{tabular}{l} b4bfcc3a-db2c-424c-b029-7fe99a87c641} \end{tabular} \label{thm:local-prop}$

Queries value:

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

Oueries value:

Oueries value:

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

Queries value:

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

Oueries value

 $\label{lem:hklmsoftware} 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:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

 $\label{thm:local-state} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \begin{tabular}{l} b4bfcc3a-db2c-424c-b029-7fe99a87c641} [stream] \end{tabular}$

Queries value:

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

Queries value:

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

Oueries value:

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

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:

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

Queries 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:

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

Queries value:

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

Oueries value

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

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[infotip]

Oueries value:

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

Queries value:

 $H\dot{L}M\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[icon]

Queries value:

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

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:

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

Queries value

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries 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:

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

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

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value

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

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folds 65f9-4cf6-a03a-e3ef65729f3d \cite{lem:hklmsoftware} \end{folder} folds \cite{lem:hklmsoftware} folds \cite{lem:hklmsoftware} \end{folder} folds \cite{lem:hklmsoftware} folds \cite{lem:hklmsoftware} \cite{lem:hklmsoftware} \cite{lem:hklmsoftware} \cite{lem:hklmsoftware} folds \cite{lem:hklmsoftware} \cite{$

Oueries value:

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

Oueries value

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

Oueries value

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

Oueries value:

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

Oueries value:

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

Queries value:

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

folders[appdata]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

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:

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

Queries value:

Oneries value

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value: $HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001[profileimagepath]$

Queries value:

 $\label{lem:hcculos} HKCU software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \d5291c63-7c88-11e3-be65-806e6f6e6963 \[data]$

Queries value:

 $\label{lem:lem:hcculos} HKCU software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\mountpoints2| cpc \verb|\volume| {d5291c63-7c88-11e3-be65-806e6f6e6963} [generation]$

Queries value: $\label{thm:linear} \begin{tabular}{ll} HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[version.dll] \\ \end{tabular}$

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