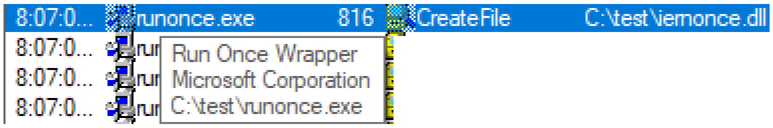
1 little known secret of runonce.exe (32-bit)

hexacorn.com/blog/2023/12/26/1-little-known-secret-of-runonce-exe-32-bit

2023-12-26

When you execute 32-bit version of *runonce.exe* on a 64-bit version of Windows and pass to it the */RunOnceEx6432* argument you will make the program load *iernonce.dll* library and execute its *RunOnceExProcess* API…

Since the *iernonce.dll* library is loaded using *LoadLibraryW* we can simply copy *runonce.exe* to a different folder, and run it from there. This will load the *iernonce.dll* library we can control…



```
8:07:0...  runonce.exe   816  CreateFile    C:\test\iernonce.dll
8:07:0...  rur  Run Once Wrapper
8:07:0...  rur  Microsoft Corporation
8:07:0...  rur  C:\test\runonce.exe
```