

[Home](#) [Services](#) [Products & Freebies](#)

[Case Studies](#) [Contact Us](#)

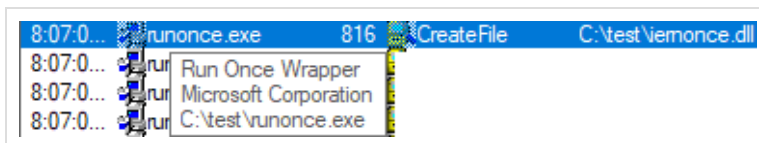
Posted on [2023-12-26](#)

[← Previous](#) [Next →](#)

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

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...



This entry was posted in [Living off the land](#), [LOLBins](#), [Threat Hunting](#) by [adam](#). Bookmark the [permalink](#).

[Privacy Policy](#) | Proudly powered by [WordPress](#)