PSBits/NoRunDll at master · gtworek/PSBits

By gtworek

Archived: 2026-04-05 21:59:26 UTC

Simple proof of concept and demonstration of RunDll32.exe limitations (a.k.a. "it's by design"). The solution consists of 3 components:

1. DLL - simple DLL exporting two methods, including "RunMe()" which is what you want to call,
2. PowerShell script calling the method you want,
3. cmd script with RunDLL32 trying to call the same method but effectively calling another one.

DLL comes in C and in compiled version - your choice.

The behavior you can observe is "by design", not very-well-known way of working of RunDll32: When you call Method() it tries to call MethodW() and MethodA() first instead of the one you asked.

And the conclusion is "Luke, use the for^H^H^H PowerShell!"

Source: https://github.com/gtworek/PSBits/tree/master/NoRunDll