GitHub - OmerYa/Invisi-Shell: Hide your Powershell script in plain sight. Bypass all Powershell security features

By OmerYa

Archived: 2026-04-06 01:14:51 UTC

Hide your powershell script in plain sight! Invisi-Shell bypasses all of Powershell security features (ScriptBlock logging, Module logging, Transcription, AMSI) by hooking .Net assemblies. The hook is performed via CLR Profiler API.

Work In Progress

This is still a preliminary version intended as a POC. The code works only on x64 processes and tested against Powershell V5.1.

Usage

- Copy the compiled InvisiShellProfiler.dll from /x64/Release/ folder with the two batch files from the root directory (RunWithPathAsAdmin.bat & RunWithRegistryNonAdmin.bat) to the same folder.
- Run either of the batch files (depends if you have local admin privelledges or not)
- Powershell console will run. Exit the powershell using the exit command (DON'T CLOSE THE WINDOW) to allow the batch file to perform proper cleanup.

Compilation

Project was created with Visual Studio 2013. You should install Windows Platform SDK to compile it properly.

Detailed Description

More info can be found on the DerbyCon presentation by Omer Yair (October, 2018).

Credits

- CorProfiler by .NET Foundation
- Eyal Ne'emany
- Guy Franco
- Ephraim Neuberger
- Yossi Sassi
- Omer Yair

Source: https://github.com/OmerYa/Invisi-Shell