Sign in

matterpreter / DefenderCheck Public

Notifications | Fork 395 | Star 2.3k

Code | Issues 2 | Pull requests 2 | Actions | Projects | Security | Insights

master | Go to file | Code

- DefenderCheck
- .gitattributes
- .gitignore
- LICENSE
- README.md
- demo.gif

About

Identifies the bytes that Microsoft Defender flags on.

csharp | research-tool | evasion

- Readme
- BSD-3-Clause license
- Activity
- 2.3k stars
- 43 watching
- 395 forks

Report repository

Releases

No releases published

Packages

No packages published

Languages

● C# 100.0%

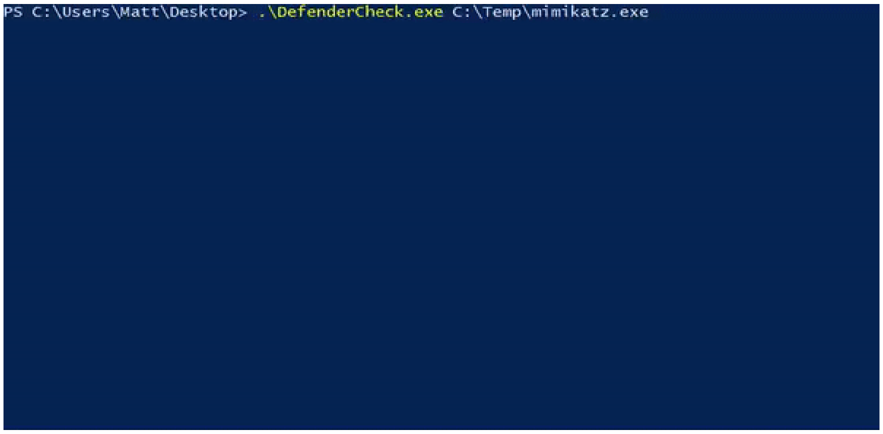
README | BSD-3-Clause license

DefenderCheck

Quick tool to help make evasion work a little bit easier.

> **Warning:** As of the 1.337.157.0 Defender signature update, DefenderCheck is classified as VirTool:MSIL/BytzChk.C!MTB. As a workaround while I work to get around this, please disable Real-time Protection in Defender before compiling DefenderCheck.

Takes a binary as input and splits it until it pinpoints that exact byte that Microsoft Defender will flag on, and then prints those offending bytes to the screen. This can be helpful when trying to identify the specific bad pieces of code in your tool/payload.



```
PS C:\Users\Matt\Desktop> .\DefenderCheck.exe C:\Temp\mimikatz.exe
```

Note: Defender must be enabled on your system, but the realtime protection and automatic sample submission features should be disabled.