


Product ▾ Solutions ▾ Resources ▾ Open Source ▾ Enterprise ▾ Pricing

🔍

Sign in

Sign up

 bats3c / EvtMute

Public

🔔 Notifications

🍴 Fork 50

★ Star 261

<> Code

🕒 Issues 1

🔗 Pull requests

🎬 Actions

📁 Projects

🛡 Security

📊 Insights

🔗 master ▾


🔗

📁

🔍

Go to file

<> Code ▾

 bats3c Merge pull request #2 from HansMartin/win7-s... 🗨 b618de7 · 3 years ago 🕒 17 Commits

📁 EvtMute	adjust the byte pattern for the Window...	3 years ago
📁 EvtMuteBin	sharpevtmute working	4 years ago
📁 SharpEvtMute	For Windows 7, use RtlCreateUserThre...	3 years ago
📁 YaraFilters	added new filters	4 years ago
📁 img	updated README	4 years ago
📄 LICENSE	Initial commit	4 years ago
📄 README.md	update readme	4 years ago

📖 README

📄 MIT license

☰

EvtMute

This is a tool that allows you to offensively use [YARA](#) to apply a filter to the events being reported by windows event logging.

Usage

Grp the latest verison from [here](#). `EvtMuteHook.dll` contains the core functionality, once it is injected it will apply a temporary filter which will allow all events to be reported, this filter can be dynamically updated without having to reinject. I've written `SharpEvtMute.exe` which is a C# assembly that can easily run via `execute` in shad0w or `execute-assembly` in cobalt strike. I will be writing a native version in C for much better intergration with shad0w.

Disabling Logging

A trivial use case would be to disable event logging system wide. To do this we can use the following yara rule.

```
rule disable { condition: true }
```

We will need to start by injecting the hook into the event service.

```
.\SharpEvtMute.exe --Inject
```

```
PS X:\> .\SharpEvtMute.exe --Inject
SharpEvtMute by @_batsec_

[i] Found PID: 1228
[+] Injected hook
PS X:\>
```

About

Apply a filter to the events being reported by windows event logging

[blog.dylan.codes/pwning-windows-event...](#)

📖 Readme

📄 MIT license

📈 Activity

★ 261 stars

👁 13 watching

🍴 50 forks

Report repository

Releases 1

📦 EvtMute

Latest

on Sep 3, 2020

Packages

No packages published

Languages

C# 91.7%

C 7.1%

Python 0.7%

C++ 0.4%

Objective-C 0.1%

YARA 0.0%

Page 1 of 3

Community Filters

If you create some useful filters feel free to make a pull request to the `YaraFilters` directory. It would be cool to have a good collection of filters to hide common actions that everyone can benefit from