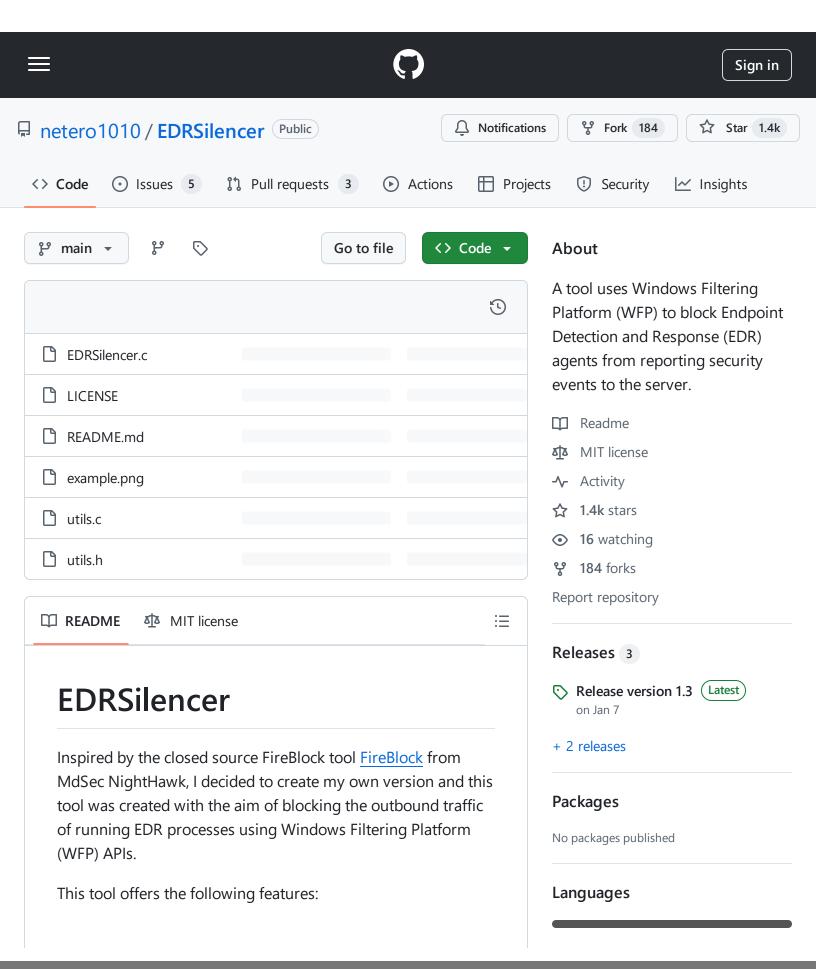
GitHub - netero1010/EDRSilencer: Atool uses Windows Filtering Platform (WFP) to block Endpoint Detection and Response (EDR) agents from reporting security events to the server. - 31/10/2024 15:48 https://github.com/netero1010/EDRSilencer



GitHub - netero1010/EDRSilencer: Atool uses Windows Filtering Platform (WFP) to block Endpoint Detection and Response (EDR) agents from reporting security events to the server. - 31/10/2024 15:48 https://github.com/netero1010/EDRSilencer

- Search known running EDR processes and add WFP filter to block its outbound traffic
- Add WFP filter for a specific process
- Remove all WFP filters created by this tool
- Remove a specific WFP filter by filter id
- Support to run in C2 with in-memory PE execution module (e.g., BruteRatel's memexec)
- Some EDR controls (e.g., minifilter) deny access when a process attempts to obtain a file handle of its EDR processes (e.g., through CreateFileW). However, the FwpmGetAppIdFromFileNameØ API, which is used to obtain the FWP app id of the targeted EDR process, calls CreateFileW internally. To avoid this, a custom FwpmGetAppIdFromFileNameØ was implemented to construct the app id without invoking CreateFileW, thus preventing unexpected failures when adding a WFP filter to an EDR process

The tool currently supports the following EDRs:

- Microsoft Defender for Endpoint and Microsoft Defender Antivirus
- Elastic EDR
- Trellix EDR
- Qualys EDR
- SentinelOne
- Cylance
- Cybereason
- Carbon Black EDR
- Carbon Black Cloud
- Tanium
- Palo Alto Networks Traps/Cortex XDR
- FortiEDR
- Cisco Secure Endpoint (Formerly Cisco AMP)
- ESET Inspect

C 100.0%

- Harfanglab EDR
- TrendMicro Apex One

As I do not have access to all these EDRs for testing, please do not hesitate to correct me if the listed processes (edrProcess in EDRSilencer.c) prove insufficient in blocking all alert, detection, or event forward traffic.

Testing Environment

Tested in Windows 10 and Windows Server 2016

Usage

Usage: EDRSilencer.exe <blockedr/block/unblocka └



- Add WFP filters to block the IPv4 and IPv6 ou EDRSilencer.exe blockedr
- Add WFP filters to block the IPv4 and IPv6 ou EDRSilencer.exe block "C:\Windows\System32\cu
- Remove all WFP filters applied by this tool: EDRSilencer.exe unblockall
- Remove a specific WFP filter based on filter : EDRSilencer.exe unblock <filter id>

Compile

x86_64-w64-mingw32-gcc EDRSilencer.c utils.c -o ☐

Example

Detect and block the outbound traffic of running EDR processes

GitHub - netero1010/EDRSilencer: Atool uses Windows Filtering Platform (WFP) to block Endpoint Detection and Response (EDR) agents from reporting security events to the server. - 31/10/2024 15:48 https://github.com/netero1010/EDRSilencer



Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information © 2024 GitHub, Inc.