



Sign in

amjcyber / EDRNoiseMaker Public



## Notifications




Fork 11



Star 76

Code


Issues

 Pull requests

## Actions

Projects

## Security

 Insights

main



Go to file

<> Code ▼

## About

## Detect WFP filters blocking EDR communications



## Readme



GPL-3.0 license



## Activity



76 stars



1 watching



11 forks

## Report repository

## Releases

No releases published

## Packages

No packages published

## Languages



# EDRNoiseMaker

## Detect WFP filters blocking EDR communications

The aim of this tool is to detect potential silencers of an EDR (or the process you choose). Based on the attack against EDR developed by [EDRSilencer](#) and [FireBlock](#), `EDRNoiseMaker` tries to detect them by checking a list of executables that have been *silenced* using the Windows Filtering Platform (WFP).

**WFP**

The Windows Filtering Platform (WFP) is a set of application programming interfaces (APIs) and system services provided by Microsoft in Windows operating systems. It is a

comprehensive networking platform that allows developers to implement custom network security solutions, packet filtering, and network monitoring applications. With WFP you are able to block network connections of a process without a very limited footprint: No registry keys, no rules added to Windows Firewall and no by default Events. This makes it a really nice approach to cut communications between EDR and the cloud console making analyst blind to what is happening there.

## Detection approach

There is no native way to list and interact with WFP. To do that we need to use the [NtObjectManager](#) module.

With the help of `NtObjectManager` we will be able to list all filters and the approach will be:

- Create a list with the executables you want to check
- Listed filters that block connections
- Filter that list by the executables provided


The actual executable list is based on the list provided by [EDRSilencer](#):

```
"MsMpEng.exe", "MsSense.exe", "SenseIR.exe", "SenseI" 
```

Add executables as you need.

## Testing

For testing purposes we will block the built in Microsoft Defender Antivirus `MsMpEng.exe` :

```
.\EDRSilencer.exe block "C:\Program Files\Windows" 
```

Then we execute `EDRNoiseMaker.ps1` and we get:

Executable



-----

```
\device\harddiskvolume3\program files\windows de  
\device\harddiskvolume3\program files\windows de
```

To remove the filters:

Import-Module NtObjectManager



\$engine = Get-FwEngine

Remove-FwFilter -Engine \$engine -Id <Id>

## Sources

I couldn't make this without this resources:

- [What The Filter \(WTF\) is Going on With Windows Filtering Platform \(WFP\)?](#)
- [EDRSilencer](#)
- [NtObjectManager](#)
- [CRWD-HBFW](#)

[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)



© 2024 GitHub, Inc.