

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.

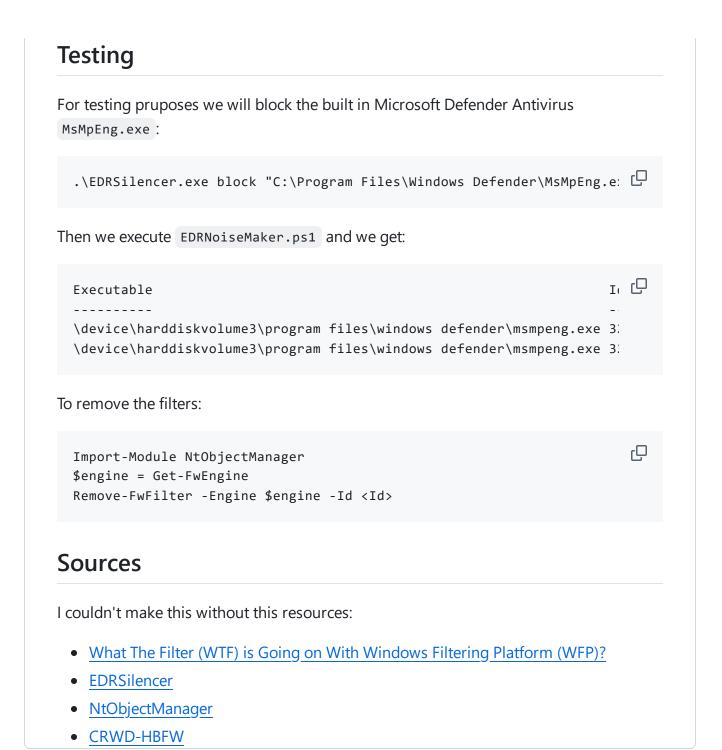
With the help of NtObjectManager we will be able to list all filters and the approach will be:

- 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","SenseNdr.exe","SenseCncPrd

Add executables as you need.



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