Branch: master

Find file Copy path

PSBits / WinDefend / README.md

gtworek polishing

2c24c38 3 days ago

1 contributor

Raw Blame History

13 lines (10 sloc) 1.16 KB

The PoC described below is 100% harmless and you can easily run it on your computer. No harm by eicar test file, no harm by exe you compile on your own from 3-lines-long source code.

It looks like realtime scanning by Windows Defender depends on the executable file name. YES, only the name, and nothing else.
Here you can prove it:

1. Copy the provided getfile.cs file to your machine.
2. Compile it with `C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe /out:getfile.exe getfile.cs`
3. Try to run resulting .exe and observe that eicar.com test file is downloaded and then immediately detected and quarantined.
4. Compile the same source providing different output file name: `C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe /out:msiexec.exe getfile.cs`

5. Launch msiexec.exe you have just created and observe eicar.com staying undetected.

If you need more info about eicar.com - see the European Institute for Computer Antivirus Research webpage: http://2016.eicar.org/85-0-Download.html

I have played on the Windows ver. 10.0.18362.476 / Defender ver. 4.18.1910.4 / Definitions ver. 1.305.2045.0. Thanks @Phenomytian for reminding me about adding this info.