

Forum:[Hack Forums](#)

Thread: [PYTHON PYINSTALLER AND VIRUSTOTAL SCAN](#)

theprogamer20 - April 24, 2019, 6:14 pm

Hello, guys am new here and i hope to meet a lot of more cool people as i venture into the hacking world.

THis is my first post please show some love

Well, i have been in the social engineering game for a while now and although i started recently learning python, i still refer to myself as a script kiddie.

But one thing stands out and that is the current hatred virustotal.com has for any python executable.

even if you create a simple python script that (print("hello world")) to the console. it would usually get flagged as a virus by at least 8 of 60 AVS on the website.

Please is there any possible way to evade the detection.

The exes were compiled with pyinstaller just in case...

Cooooool - April 24, 2019, 6:22 pm

Simple! Stop fucking scanning on virustotal. Literally the worst thing you could ever do on Hackforums. I have seen some way to do with signing or something. I actually can't really remember right now, I just came here to tell you to stop using virustotal.

Faith Connors - April 24, 2019, 9:49 pm

(Apr 24, 2019 06:22 PM)Cooooool Wrote: [\[CITE\]](#) Simple! Stop fucking scanning on virustotal. Literally the worst thing you could ever do on Hackforums. I have seen some way to do with signing or something. I actually can't really remember right now, I just came here to tell you to stop using virustotal.

he said he was only scanning hello world.

although he shouldn't scan his malware on vt, that doesn't mean that someone else won't scan it there.

the easy answer to op's query is to just use a different language. python isn't really good for malware dev since it's incredibly difficult to run python code on a target machine unless they have python installed. but if they have python installed, they'll probably check the script before running it, so that's another issue. pyinstaller/py2exe might sound like a decent solution, but considering that hello world drops a 5mb .exe, you'll quickly realize that it's another bad idea. write the same thing in c/c++ or even rust or go and your filesize will immediately drop to a few KB at most.

on top of this, with native development, your code will run just about anywhere as long as you compile it properly. it'll also get around most av detection as long as you actually write your own code and don't leech others too hard. no crypter needed, just be smart.

as for code signing, there definitely is a correlation and i actually wrote a thread not too long ago on

the subject:

<https://hackforums.net/showthread.php?tid=5955770>

CyberStrike - April 25, 2019, 11:10 am

Veil fucked you hard, it uses pyinstaller cx_freeze and py2exe will have a little less detections but still Veil really has done a number on python and pyinstaller when it comes to detections.