

Forum:[Hack Forums](#)

Thread: [How to make a python reverse shell FUD when changed to exe?](#)

DrollBeack18100 - February 5, 2018, 3:32 am

How to Change py to exe? (I tried with py2exe and pyinstaller but they always change the code and no connection received)

How to make a python reverse_shell Fully Undetectable by all antiviruses?

What makes the payload FUD against the antivirus , like if i changed the code but its output will be the same? Or i must encrypt it?

Sorry for asking too much questions , i searched alot and i found that hackforums is better than Google.....

Ri?dle - February 5, 2018, 4:11 am

I could be wrong, but I think no very known library like py2exe would make a python malware FUD

DrollBeack18100 - February 5, 2018, 4:30 am

(Feb 5, 2018 05:11 AM)Ri?dle Wrote: [\[CITE\]](#) I could be wrong, but I think no very known library like py2exe would make a python malware FUD

i didn't mean that though too . ? . No probs , thank you :).

I mean the py2exe changes something in the code so it gives error.

TheWarOwl - February 5, 2018, 1:53 pm

You also can do some basic obfuscation on your code. That or change little things in how it works and see if your detections go down.

Freaki - February 5, 2018, 1:54 pm

use pyinstaller my friend but its basically worthless since your stub will be 10 megabytes XD

DrollBeack18100 - February 6, 2018, 2:04 pm

I'm on kali linux whenever i do pyinstaller file.py , it doesn't give me file.exe

Ri?dle - February 6, 2018, 7:28 pm

(Feb 6, 2018 03:04 PM)DrollBeack18100 Wrote: [\[CITE\]](#) I'm on kali linux whenever i do pyinstaller file.py , it doesn't give me file.exe

um.. py2exe wont work on linux, you can't even run a .exe on linux without doing some special shit

DrollBeack18100 - February 7, 2018, 1:14 am

(Feb 6, 2018 08:28 PM)Ri?dle Wrote: [\[CITE\]](#) um.. py2exe wont work on linux, you can't even run a .exe on linux without doing some special shit

i know this , but pyinstaller changes py to something weird not exe..

monarch6 - March 3, 2020, 5:07 am

(Feb 6, 2018 03:04 PM)DrollBeack18100 Wrote: [\[CITE\]](#) I'm on kali linux whenever i do pyinstaller file.py , it doesn't give me file.exe

lol use wine

(Feb 6, 2018 03:04 PM)DrollBeack18100 Wrote: [\[CITE\]](#) I'm on kali linux whenever i do pyinstaller file.py , it doesn't give me file.exe

you will want to install pyinstaller with python3.7 in wine... then u shouldnt have any problems... other than the fact that pyinstaller will get flagged by most av now (thanks to fucking vt)

Morphine - March 6, 2020, 12:20 pm

I am working on a python Crypter which takes the native/.net executable and encrypt and obfuscate and make the stub output .exe size 5mb and FUD 0/35 Scantime, Runtime its not avaiable as i am working on solution of it!

omar18881 - March 21, 2020, 11:55 pm

(Feb 5, 2018 02:54 PM)Freaki Wrote: [\[CITE\]](#) use pyinstaller my friend but its basically worthless since your stub will be 10 megabytes XD

(Mar 3, 2020 06:07 AM)monarch6 Wrote: [\[CITE\]](#) lol use wine

you will want to install pyinstaller with python3.7 in wine... then u shouldnt have any problems... other than the fact that pyinstaller will get flagged by most av now (thanks to fugging vt)

To Freaki , the stub isn't going to be 10 Megabytes Minimum Size with pyinstaller is 5.6 Mega Bytes , it was with Pyinstaller 3.6 with python 3.6.0 , it was python/meterpreter/reverse_tcp

AntiScan Result:

Spoiler [\(Click to View\)](#)

My Vimeo Video:

Spoiler [\(Click to View\)](#)[Video: <https://vimeo.com/398143452>]

That is the Best Approche you can do to make it Exe with Python, the size of any pyinstaller executable is depending totally on the imports you are giving , for example if you imported any preinstalled modules like base64 or os , sys , etc it won't effect the size that much , but if you imported PyQt5 (which you will need to install via PIP) the size will start go Crazy , to me size from 5~10 Megabytes is a Disadvantage but what about the advantage , well you code Malware extremely Fast ,and for making it FUD and not flagged Trust me it's much easier than you think , the way pyinstaller work is long road for the anti-virus to detect it , i can bet you right now to add me on discord and you will see me compiling the Source Code of reverse_tcp payload WITHOUT ANY KIND OF ENCRYPTION AND ENCODING and i will bybass AVAST Scantime and Runtime, why you ask because the way pyinstaller works it get's the interpreter and your modules and the script all in one big ZlibArchive and put all that in bootloader Coded in C , So when you run the bootloader © program extract the ZlibArchive(script & modules & interpreter) and run the script using the interpreter , you can check the pyinstaller documentary for more , so it's much easier to bybass the anti-virus in Python executable , so no it won't detected by anti-virus at all, just know what you are doing, and trust me 5~10 mb isn't that bad , and one more thing the pyinstaller executable are C program it will work from windows 7~10 no dependencies needed ?,

Check My Tool i will Update it Soon ,

totally in Python : <https://hackforums.net/showthread.php?tid=6058000&mode=single>