

Forum:[Hack Forums](#)

Thread: [Making a crypter](#)

Kisame? - December 18, 2016, 8:10 am

Hello,

I've recently been looking into crypters and how they work and I'd like to create something myself. This is the idea I've got on how crypters work, correct me if I am wrong;

The payload first gets encrypted with a chosen encryption method (for example AES). This makes the file unlockable with a password/key. This means AV's won't be able to say it's a virus if it gets scanned since they cannot see what's inside the encrypted file.

However, to run, the file needs to be decrypted. That is why there is a stub added to the encrypted file. This is basically a piece of code which contains the code and decrypts the payload on runtime so it can properly run.

The payload and stub both get injected in a .exe, which executes the stub and thus the payload on execution .

Am I wrong somewhere?

I'd love to make my own crypter. Well, it doesn't have to be my own crypter. Making an open-source crypter FUD or nearly FUD would be perfectly fine.

If anyone has experience with this, I'd like to learn and if someone has any tips, feel free to add me @skype, kisuke_urahara.bl.

I don't know a lot about coding tbh, I thought it would be the best to maybe start learning regular C. I believe that's the easiest to pick up?

However, I have no idea where to start about the crypter :s

Any help is appreciated,
Thanks in advance. ?

xHeaven - December 18, 2016, 8:43 am

Quote:I have no idea where to start about the crypter :s

Download source codes from anywhere and try to learn from the source. This is the best way, I think.

Kisame? - December 18, 2016, 8:45 am

(Dec 18, 2016 09:43 AM)xHeaven Wrote: [CITE](#) Download source codes from anywhere and try to learn from the source. This is the best way, I think.

Will do that for sure, thanks :)

Arrogance - December 19, 2016, 5:01 am

First learn any desktop application programming language then jump into crypters.

Kisame? - December 19, 2016, 6:49 am

(Dec 19, 2016 06:01 AM)Arrogance Wrote: [\[CITE\]](#) First learn any desktop application programming language then jump into crypters.

That'd maybe be necessary indeed..

Is C a good start?

Arrogance - December 19, 2016, 11:01 am

(Dec 19, 2016 07:49 AM)David? ?Gilmour Wrote: [\[CITE\]](#) That'd maybe be necessary indeed..

Is C a good start?Surely. C is the base of all languages.

Kisame? - December 20, 2016, 2:30 am

(Dec 19, 2016 12:01 PM)Arrogance Wrote: [\[CITE\]](#) Surely. C is the base of all languages.

I'll look into it once I've got some time (probably @ the end of the week).

Thanks for your support.

Codefuser - December 20, 2016, 4:30 am

Learn to code first. It is hard to understand how a crypter works without at least knowing how to code, PE structure, etc

Donkey Death Jam - December 20, 2016, 4:33 am

There was a good thread that someone posted on here a while back. You don't have to learn it all, but the basics are all taught there.

[Click here to view the thread](#)

(Dec 20, 2016 05:30 AM)Codefuser Wrote: [\[CITE\]](#) Learn to code first. It is hard to understand how a crypter works without at least knowing how to code, PE structure, etc

First thing you should do is just code a basic crypter using a public RunPE, it'll be detected but doing that will give you the basic idea of how a crypter works. Then you can research about the PE header structures and develop your own RunPE.

Codefuser - December 20, 2016, 4:59 am

(Dec 20, 2016 05:33 AM)Donkey Death Jam Wrote: [\[CITE\]](#) There was a good thread that someone posted on here a while back. You don't have to learn it all, but the basics are all taught there.

[Click here to view the thread](#)

First thing you should do is just code a basic crypter using a public RunPE, it'll be detected but doing that will give you the basic idea of how a crypter works. Then you can research about the PE header structures and develop your own RunPE.

True, but your experience with it will be much better when you know the basic.

theperson - December 20, 2016, 10:28 am

To answer your question about what language to learn first. I would suggest C if coding a Crypter is all you want to accomplish. But, if you are interested in learning from the beginning and want a suggestion of what would be easy to start with, Python is the way to go in my opinion. The concepts are easier to understand, it is more simplified, and you wouldn't be as frustrated because there is less to learn before you see results. Good luck, and don't get discouraged when you fail. Especially when coding in C, segmentation faults can be a huge headache. Also the learning curve for memory management, and the structure of C can be steep for most people.

Kisame? - December 20, 2016, 11:10 am

Thanks for all answers, I appreciate it a lot.

Think I will look into C and then look into creating my own runPE!