

Forum:[Hack Forums](#)

Thread: [Software Code Encryption](#)

Sofia_Paradise - January 6, 2020, 4:10 am

Hi guys, I kinda have some knowledge (not complete noob), but I am having troubles to understand how the encrypted .exe files work.

The thing that confuses me is this scenario:

1. You have some malicious code that you want to make FUD.
2. Lets say that you crypted it successfully and its not detected.

And now the questions start:

How the computer understands what is it coded in this encrypted code?

How the code is decrypted to the PC without alerting the AV programs ?

As far as I understood usually the decryption code is somehow hidden in the code?

Would be very thankful if someone clarify this for me! ?

Meterpreter - January 6, 2020, 4:18 am

The obfuscated code is still actual code, it is still technically readable, its just much harder to reader. The stronger the obfuscation, the slower the program (usually), because you're adding more and more layers.

In the end it always ends up as machine code.

Sofia_Paradise - January 6, 2020, 4:27 am

(Jan 6, 2020 05:18 AM)Sys Wrote: [\[CITE\]](#) The obfuscated code is still actual code, it is still technically readable, its just much harder to reader. The stronger the obfuscation, the slower the program (usually), because you're adding more and more layers.

In the end it always ends up as machine code.

Thank you for the fast reply!

Okay if we say that I want to try building own crypter, how is the encryption working(does it mess with the bytes or it is just transforming the code in other "form"?).

Maybe the correct question is "What are those layers doing with the code?".

At this point I understand that maybe the best thing is to learn more about cryptography, but would be great to find some answers here also ?

FuzzylInteger - January 6, 2020, 11:17 am

(Jan 6, 2020 05:10 AM)Sofia_Paradise Wrote: [\[CITE\]](#) How the computer understands what is it coded in this encrypted code?

How the code is decrypted to the PC without alerting the AV programs ?

As far as I understood usually the decryption code is somehow hidden in the code?

Would be very thankful if someone clarify this for me! ?

1) the computer just execute command, so there is nothing to "understand", so the cpu will start to execute the code until the code end, when the code end the routine are executed

2) the code is most of the time decrypted in memory "because is faster", the av will not scan the memory so often, but nowadays modern av scan memory when some action are taken, so yes the av can detect the code even if is decrypted in memory ;)

3)the decryption code, is CODE so it's executed like other routine, if you have the decryption key u can read the output