Forum:Hack Forums

Thread: Simple way to encrypt raw exe data?

zeller0 - *December 28, 2018, 7:29 pm*

Hi all,

I'm writing a RunPE. I'm storing the applications raw data in the program by using HxD and copying it all with 'C'.

This is what it looks like:

Code unsigned char zcpx[size] = {
    0x4D, 0x5A etc...
};
I was wondering if there was a simple way to encrypt this data to bypass an AV. Without the raw data in the application, the RunPE's already FUD (scantime and [runtime with non-malicious application]).

Cheers.

Xamarin - *December 29, 2018, 9:43 am*

The simplest way is by applying a technique to the data like the Caesar Cipher. So basically you can "encrypt" it by adding a number to all those bytes to get a new result. So for example, if you have a byte 0x4F(hex) and you decided to use 15(dec) as your shifting key, then 0x4F will become 0x5E. That way you will create what it will seem "garbage data". One better approach would be to deploy encryption and decryption techniques to the executable itself. So for example, you will have statically encrypted parts of your code, and you will decrypt them only when you need them. Of course, the road to become FUD will become quite difficult as you can understand, because the algorithms to implement the encryption/decryption as well as the deployment (which is probably the hardest part to FUD) of the "program" need to be implemented in a unique way that will not trigger any kind of heuristic detection. Anyways, you have still a lot of road ahead of you. GLHF.

Hoodie+ - *December 29, 2018, 10:47 am*

You can make somekind of XOR encryption but I am not sure how effective it will be because it may be detectable...

El Lobo - *December 29, 2018, 11:01 am*

(Dec 29, 2018 11:47 AM)Hoodie+ Wrote: *[CITE]* You can make somekind of XOR encryption but I am not sure how effective it will be because it may be detectable...
For that purpoae XoR is more than enough.

spiderfruit - *December 30, 2018, 2:05 am*

xor encryption won't be that effective since it can be easily emulated by any decent antivirus engines

El Lobo - *December 30, 2018, 5:16 am*

(Dec 30, 2018 03:05 AM)spiderfruit Wrote: *[CITE]* xor encryption won't be that effective since it can be easily emulated by any decent antivirus engines
Antiviruses dont emulate ecryption algorithms.

spiderfruit - *December 30, 2018, 6:31 am*

(Dec 30, 2018 06:16 AM)El Lobo Wrote: *[CITE]* Antiviruses dont emulate ecryption algorithms.

AV are capable of emulating your whole code and ignore any conditional jumps given, they can find your decryption routine and call it even though you didn't execute it yet that's what emulation does even if they fail emulating there's still the possibility of bruteforcing the key

El Lobo - *December 30, 2018, 8:46 am*

(Dec 30, 2018 07:31 AM)spiderfruit Wrote: *[CITE]* AV are capable of emulating your whole code and ignore any conditional jumps given, they can find your decryption routine and call it even though you didn't execute it yet that's what emulation does even if they fail emulating there's still the possibility of bruteforcing the key

Thats a different answer than the one before. They emulate the whole code and I doubt that any is bruteforcing the key. And XOR is sufficient as an encryption algorithm in av evasion. If the file is being emulated then its not important if you used AES or XOR. In av evasion, encryption is just used to break av signature.

gigajew - *December 30, 2018, 11:15 am*

I've confirmed multiple times most AVs detect simple algorithms like xor in the code and decipher it just in one scan, that's how they can throw a Quasar label on a loader with xor ciphered stub

El Lobo - *December 30, 2018, 11:27 am*

(Dec 30, 2018 12:15 PM)gigajew Wrote: *[CITE]* I've confirmed multiple times most AVs detect simple algorithms like xor in the code and decipher it just in one scan, that's how they can throw a Quasar label on a loader with xor ciphered stub

Its not a problem of the algorithm, its the implementation of it. They emulate the file and see that unecrypted version is quasar and thus label it as such. They in no way just decrypt the random shit and try to gusss the algorithm or bruteforce the key.

zeller0 - *December 30, 2018, 9:45 pm*

(Dec 30, 2018 12:15 PM)gigajew Wrote: *[CITE]* I've confirmed multiple times most AVs detect simple algorithms like xor in the code and decipher it just in one scan, that's how they can throw a Quasar label on a loader with xor ciphered stub

I can second this. Using something as simple as xor to encrypt the stub gave me detections for babylon as well as loaders and injectors.

Something much harder to decrypt or something not as simple as a simple xor encrypt may help with these detections.

Also;

My stub went from 1/26 using a different method of encryption to 7/26 while using xor.

you_can_never_hack_me - *December 31, 2018, 12:41 am*

You don't have to encrypt it - You compare Target Data with/to Created Data n-way(s) n-time(s) and the truth starts to emerge byte by byte.

It's simple.