

Forum:[Hack Forums](#)

Thread: [What is the best Obfuscation Methods to Bypass AV's](#)

Voirus - November 14, 2023, 4:54 pm

Hello I am currently building a software to bypass AV's and I am about to implement the ofbuscation part.

Which is the best obfuscation method / github link and please explain why.

I am Looking for experienced people to give me there opinion so that I can finalize this project with sucess

Any other tips are welcome don't hesitate ?

Tentco - November 14, 2023, 6:41 pm

(Nov 14, 2023 05:54 PM)Voirus Wrote: [\[CITE\]](#) Hello I am currently building a software to bypass AV's and I am about to implement the ofbuscation part.

Which is the best obfuscation method / github link and please explain why.

I am Looking for experienced people to give me there opinion so that I can finalize this project with sucess

Any other tips are welcome don't hesitate ?

If it's .NET use light obfuscation over your final build, use AES 256 using random key & iv and base64 encode your file, don't obfuscate namespaces, classes, junk AV knows the generic obfuscation pattern, how are you bypassing the AV using implant? If yes, use DInvoke to to dynamically load API calls, one thing you could also add is erasing PE headers info at runtime(semi-polymorphic).

If it's process Injection or shellcode allocation avoid RunPE/LoadPE, use something like Callback Function.

At the End there are just lot of things to add.

The generic obfuscation goes like - bytes -> base64/AES -> bytes -> base64 then just do the reverse.

Voirus - November 15, 2023, 12:27 pm

Thanks for the answer.

When people mention they do private crypts do they do it manually for every file they work with, or did they build a software before hand and all they do is implement the file to the software which is private.

HiddenEyE - December 3, 2023, 2:48 pm

bypasing AV's requires high level of skill.

tips to help you (for educational use):

1. you cannot bypass what you dont understand how it works.
11. check for hooking and unhooking(try coding a hook and unhook engine)
111. i use for encryption and decryption method e.g blowfish,aes,xor,rsa etc but that is not everything

1V. develop techniques that is new

V. do things that AV never expected you do.(high skills mate)

etc.

(Nov 15, 2023 01:27 PM)Vovirus Wrote: [\[CITE\]](#) Thanks for the answer.

When people mention they do private crypts do they do it manually for every file they work with, or did they build a software before hand and all they do is implement the file to the software which is private.

best is manually