

Forum:[Hack Forums](#)

Thread: [Evade detection by obfuscating it](#)

Hijacker - July 13, 2024, 12:38 am

Hey, I'm here for someway to make 0 detection. I've tried many ways to do using base64 obfuscation and other. Still making even more detectable and I wanna ensure, it's not detecting by any antivirus. Have tried to virustotal and showing 40 of file threat with obfuscating, but without it's 35 detection. I'm curious, if there is way to make to 0. Maybe is there technique or way to make undetectable to av at all? Coded many ways to obf, but still detectable. Did all of this methods like using upx compress, also obfuscate partions of codes like methods, loops etc, but not all

ZLOY - July 13, 2024, 7:42 am

(Jul 13, 2024 12:38 AM)Hijacker Wrote: [\[CITE\]](#) Hey, I'm here for someway to make 0 detection. I've tried many ways to do using base64 obfuscation and other. Still making even more detectable and I wanna ensure, it's not detecting by any antivirus. Have tried to virustotal and showing 40 of file threat with obfuscating, but without it's 35 detection. I'm curious, if there is way to make to 0. Maybe is there technique or way to make undetectable to av at all? Coded many ways to obf, but still detectable. Did all of this methods like using upx compress, also obfuscate partions of codes like methods, loops etc, but not all

Base64 is not obfuscation but an encoding format. When a scanner sees base64 it will decode it and detect what is being encoded. The solution is to crypt using private crypter and stub where the stub is not shared with other people.

Also, if you send the file to a service that include scanner that flags all unsigned files, you will never get full score. But that is not a problem.

DramaKing - July 13, 2024, 8:25 am

AVs today will decode base64, decompress compressed code, perform heuristic analysis, and reverse other types of obfuscation. Finding techniques that work on every type of AV known to a scanner is practically unheard of. Even then, most AVs send samples for manual analysis of any code that is unknown. In a few days or possibly weeks, the malware will no longer be FUD.

Hijacker - July 13, 2024, 12:05 pm

What about other encryption obfuscate to make random language including: Kurdish, Chinese, Japanese, Arabian. Could this decrypt easily with my own programming algorithm made obfuscation in utf-8. I've being testing and also AV is checking your behavior, so it could detect, potentially block that virus easily, maybe if it is slight chance, when in kernel mode to exclude to av, after running it. Still researching the solution

DramaKing - July 13, 2024, 2:12 pm

(Jul 13, 2024 12:05 PM)Hijacker Wrote: [\[CITE\]](#) What about other encryption obfuscate to make random language including: Kurdish, Chinese, Japanese, Arabian. Could this decrypt easily with my own programming algorithm made obfuscation in utf-8. I've being testing and also AV is checking your behavior, so it could detect, potentially block that virus easily, maybe if it is slight chance, when in kernel mode to exclude to av, after running it. Still researching the solution

Even if the language accepts multilanguage naming, the code still has to be compiled. You'd still want it to do malicious things.

Code has to run in order to abuse the kernel.

secret_code - July 14, 2024, 12:36 am

(Jul 13, 2024 02:12 PM)DramaKing Wrote: [\[CITE\]](#) Even if the language accepts multilanguage naming, the code still has to be compiled. You'd still want it to do malicious things.

Code has to run in order to abuse the kernel.

will try to help you, but 90% sure nothing will actually help you out unless someone is there near you looking at your code.

others have already said that but base64 is not obfuscation, is encoding. if you want to obfuscate you first need to understand the difference between obfuscation and encoding. if you think obfuscation is key, you're going down a rabbit hole... my questions would be, do you perhaps have any other existing malware sample within your code that might compromise your one? What is the frequency of sys calls within your code? Is there any string in your code that might raise red flags? i show you some examples of what some "suspicious" strings might look like so you can have an idea about it:

"C:\Windows\System32"

"system.ini"

"cmd.exe"

... etc

function names also can raise red flags, functions like CreateProcess, WinExec, ShellExecute etc...

since you mentioned that you actually encoding with base64, i also need to point out that encoding with base64 in 2024 is actually not very recommended, when AV engine gets into a base64 shit it will just blast the shit out of it, also applies for hex and xor encoding as well, it is too easy and suspicious to use... just use AES-256 or RSA, they are not easy to decrypt(i mean impossible almost) so AVs will think that it is just advanced encryption used for encrypting sensitive data and will bypass that, also because there is no way for the AV engine to decrypt something encrypted with RSA or AES 256 block size schemes, they would need a quantum motherfucker computer to have it decrypted, and it will not happen...

Another problem might be Network related string or function calls like socket, bind, connect ,send, recv etc... or hardcoded URL addresses or IPs(especially those known for malicious activities). Other strings include those related to privilege escalation or security bypasses(this get detected by heuristic analysis mostly as they're network related).

as you can see there are literally 1000s of ways Avs will detect your stuff, and that was not even the tip of the iceberg, there are lot more... you might be careful with naming conventions and hardcoded strings, because even if you encode your stuff with b64 the AV engine will literally spend i nanosecond to detect the encoding format and decode it, eventually leading to your real strings, and if those contain what i've said above, then your toasted, let's not forget today AV engines also use AI to scan files. I don't know what you're trying to do here, if you're using a dropper, staged droppers or other techniques to inject your malware, but i might suggest an easy and quick solution for you if file size is not a problem, you can try to make it bigger then 8mb , add some common code(code that looks just like normal code, eg: a snake game), add it to the beginning of your file, and at the very end of the file, add your actual code, while scanning the file, the AV will see your useless snake game instead of the malicious code, and since the file is >= 8MB, the AV also will skip full scan, eventually will break out at half of the file, leading to the rest of the code being undetected because the AV is fucking lazy, if you're asking why it would skip or not fully scan your file because is too big the reason is "scanning timeout", almost every AV engine has a timeout for a scan, it will break the scan and only partially scan a file if it exceeds +-8MB, usually malware is not that big, so they will think is a legitimate file, also because they can't afford to spend to much time on a single scan... in other words, you need to think out of the box if you want to evade AV detection

nowdays... don't get stuck on just base64 encoding your stuff, it will fail!

Hijacker - July 14, 2024, 3:15 am

I made something like this to change variables, obj names, names, methods etc. This is running with exec. Have tried many more ways

https://www.mediafire.com/view/8ymu02invv8ftnh/Screenshot_%252829%2529.png/file

Try to maximize way using upx everything to make it even harder, because upx helps it seems. I got my program that is named as fake svchost.exe to make undetectable to user interface, have been fiddling with manifest version to configurate. Btw I know what is encoding. It seems, when obfuscating everything make more detectable or otherway I test, what is generally less detectable, but can code encryption in AES to make CBC mode or something similar with secret_key, that is using xor mechanism. I'm coding to combine mapping with AES encryption

I've been testing and it really helps obfuscation with mapping + aes. The virus has literally bypasses a lot of detections

secret_code - July 15, 2024, 3:23 am

(Jul 14, 2024 03:15 AM)Hijacker Wrote: [\[CITE\]](#) I made something like this to change variables, obj names, names, methods etc. This is running with exec. Have tried many more ways

https://www.mediafire.com/view/8ymu02invv8ftnh/Screenshot_%252829%2529.png/file

Try to maximize way using upx everything to make it even harder, because upx helps it seems. I got my program that is named as fake svchost.exe to make undetectable to user interface, have been fiddling with manifest version to configurate. Btw I know what is encoding. It seems, when obfuscating everything make more detectable or otherway I test, what is generally less detectable, but can code encryption in AES to make CBC mode or something similar with secret_key, that is using xor mechanism. I'm coding to combine mapping with AES encryption

I've been testing and it really helps obfuscation with mapping + aes. The virus has literally bypasses a lot of detections

good, don't use xor, xor is easy to reverse, and combining it with AES is just futile, AES itself is enough...

Uolcan - July 15, 2024, 3:53 am

(Jul 13, 2024 08:25 AM)DramaKing Wrote: [\[CITE\]](#) AVs today will decode base64, decompress compressed code, perform heuristic analysis, and reverse other types of obfuscation. Finding techniques that work on every type of AV known to a scanner is practically unheard of. Even then, most AVs send samples for manual analysis of any code that is unknown. In a few days or possibly weeks, the malware will no longer be FUD.

I think you didn't hear about the new maleware tech that have 100% FUD , the stub installl tor service + open directory on victim pc ... no UAC no Smartscreen no anything i tested it my self after i write a showcase for video i watched on russian forum

DramaKing - July 15, 2024, 4:36 am

(Jul 15, 2024 03:53 AM)Uolcan Wrote: [\[CITE\]](#) I think you didn't hear about the new maleware tech that have 100% FUD , the stub installl tor service + open directory on victim pc ... no UAC no Smartscreen no anything i tested it my self after i write a showcase for video i watched on russian forum

Yeah, good one. ?