

Forum:[Hack Forums](#)

Thread: [trying to reverse engineer malware](#)

tamika-b - September 18, 2024, 10:45 am

found a batch file that seems to have aes encryption i just couldnt understand how it even works, and im wondering if there are guides that explain malware encryption/obfuscation in detail, thanks

Delfin - September 18, 2024, 11:27 am

(Sep 18, 2024 10:45 AM)tamika-b Wrote: [\[CITE\]](#) found a batch file that seems to have aes encryption i just couldnt understand how it even works, and im wondering if there are guides that explain malware encryption/obfuscation in detail, thanks

Batch files can't really have AES encryption, or any encryption at all really, without PowerShell. If I had to guess, it was obfuscated using Somalifuscator, an advanced Batch obfuscator on github. You could post a screenshot of what it looks like, and I might be able to tell you if it's Somali. There was a deobfuscator for Somali released I believe, but I don't know where

tamika-b - September 18, 2024, 11:49 am

this is the beginning: [i.imgur.com/HRdp0I9 \(dot\) png](https://i.imgur.com/HRdp0I9.png)

this is the very end: [i.imgur.com/Rj2foH5 \(dot\) png](https://i.imgur.com/Rj2foH5.png)

i had line wrap in notepad++, the script has 450,000 lines. i figured its encrypted because when i run it it executes a cmd or as u suggested powershell i noticed it executes instructions that mentions AES, key and IV. i think the key was encoded in base64. [i.imgur.com/bwNPGav \(dot\) png](https://i.imgur.com/bwNPGav.png)

Bastille - September 18, 2024, 11:50 pm

Mmmmmh, maybe something more like obfuscation than encryption, it's quite common to see obfuscated code to make the analysis less trivial, but I'm not really comfortable with this field for the time being

[M?tt](#) I know that you recently were into "hash / encryption" stuff; do you have an idea maybe ? [DramaKing](#) you replied to Matt's thread, I'm tagging you in case you could bring us some info, I'm interested by this topic, sorry for the disturbing :p

DramaKing - September 19, 2024, 4:17 am

I thought I knew obfuscation and PowerShell encryption, but this is really sophisticated.

Tha Sneak - September 19, 2024, 6:06 am

In my opinion it probably builds and executes .vbs scripts as well as call on different command line tools some popular ones are Nirsoft.

M?tt - September 19, 2024, 10:58 am

[Bastille](#)

Going to agree with [DramaKing](#) on this one. I'm not helpful at all since my inquiry was just looking for other ways to crack hashes.

ttbr0 - September 19, 2024, 6:13 pm

this doesnt look complex at all. at best it probably does some string aliasing obfuscation with

base64. i bet its also powershell because you can see namespace operators and what looks like class method invocation in the second screenshot. it will just take some time to clean up the string obfuscation if you want to do it manually. alternatively you can just run it in a vm and attempt to capture the apparent powershell using powershell logging through event logs.

edit: didnt see the third screenshot until now but having it be cleared up it looks pretty trivial to figure out. again, time is probably the only issue if you wanna do it statically and manually.

M?tt - September 19, 2024, 6:20 pm

(Sep 19, 2024 06:13 PM)ttbr0 Wrote: [\[CITE\]](#) this doesnt look complex at all. at best it probably does some string aliasing obfuscation with base64. i bet its also powershell because you can see namespace operators and what looks like class method invocation in the second screenshot. it will just take some time to clean up the string obfuscation if you want to do it manually. alternatively you can just run it in a vm and attempt to capture the apparent powershell using powershell logging through event logs.

edit: didnt see the third screenshot until now but having it be cleared up it looks pretty trivial to figure out. again, time is probably the only issue if you wanna do it statically and manually.
I probably relied too heavily on the fact that OP said it was AES.

The first screenshot looks like it could be deciphered when cleaned up, but when I'm hearing 450,000 lines I opted to give it less attention (my own fault).

I'd say you're correct in informing OP to clean up the code. There is probably a lot of garbage in there and judging by the 2nd picture, I'm guessing that's true. 2nd picture means absolutely nothing for me.

ttbr0 - September 19, 2024, 6:28 pm

(Sep 19, 2024 06:20 PM)M?tt Wrote: [\[CITE\]](#) I probably relied too heavily on the fact that OP said it was AES.

The first screenshot looks like it could be deciphered when cleaned up, but when I'm hearing 450,000 lines I opted to give it less attention (my own fault).

I'd say you're correct in informing OP to clean up the code. There is probably a lot of garbage in there and judging by the 2nd picture, I'm guessing that's true. 2nd picture means absolutely nothing for me.

450,000 lines is massive so i understand that the effort might not be worth it. part of the cause of the length might be because of the string obfuscation and it should also be known that powershell only accepts a maximum character length of 32,764 (8,191 for cmd.exe) per command.

and yes, there should also be smarter and efficient ways to reverse engineer something like this which is why i added that you can just attempt to run the script in a vm and try to log the command line arguments through event log. sysmon can also help track process creation command line arguments which could help if the built in powershell logging does not work.

notagh0st - September 19, 2024, 7:53 pm

Would you mind supplying the whole script in text format?

Edit: One thing that could be happening here is the powershell script might not be everything needed to run it, i.e. it could be that this powershell script is loaded into memory, and some other bit of code doesn't a bunch of regex replaces on the strings, and then it spawns a shell and runs it. Might not be the case, but I think if you could provide the full thing, it might become apparent

quickly.

BlackSoulZN5006 - *September 22, 2024, 6:37 pm*

What program are you using for reverse engineer malware ?