

Forum:[Hack Forums](#)

Thread: [ByteCrypter == ByteProtector V3 == Backdoor RAT](#)

Hackers - March 27, 2024, 4:41 am

Hello, I just received my purchased copy of [SIM-2362145](#) 's crypter "ByteCrypter v3".
When I inspected it, I noticed a few things.

1) Not modified since 2021. This is modern?

Spoiler [\(Click to View\)](#)

2) The hex data says it is ByteProtector V3 - Not ByteCrypter

Spoiler [\(Click to View\)](#)

3) The hex data shows a connection to Aegis 'loader & logger' - that's their bot/logs system, NOT licensing like SIM says it is.

Spoiler [\(Click to View\)](#)

4) When I opened it, it immediately tried to perform drag & drop operations, and I had 1 other failed error for an attempt to steal clipboard data. I had a locked down VirtualBox for this & if I hadn't set the permissions like this, it would've transferred files and completely f'd me.

Spoiler [\(Click to View\)](#)

5) The builder is infected

Spoiler [\(Click to View\)](#)

You can see here that he has been doing this for a while - someone else uploaded this current copy 27 days ago:

<https://www.virustotal.com/gui/file/b49bec25e7ee0e9de2004eeaef7ae1a4e509e0efa4a3618e009687c5322570d0>

More:

<https://www.hybrid-analysis.com/sample/b49bec25e7ee0e9de2004eeaef7ae1a4e509e0efa4a3618e009687c5322570d0>

https://www.kleenscan.com/scan_result/988baf9e6117d3648796d64fb232d0dc296d298b8110a13b594a17397b064c80

6) Sketchy behavior logs - Takes a screenshot for example
Spoiler ([Click to View](#))

Please check the following threads for more information about ByteCrypter from SIM-2362145 & the associated Aegis logger/scanner/crypter tool:

<https://hackforums.net/showthread.php?tid=6263240>

<https://hackforums.net/showthread.php?tid=6264915>

<https://hackforums.net/showthread.php?tid=6262966>

[SIM-2362145](#)

Please tell me why you are backdooring HF users - your own customers... Why would you do this?

ScrubspooF - March 27, 2024, 4:50 am

Hasn't this guy been closed like 5 times now?

Euaggelistes - March 27, 2024, 4:52 am

Thank you so much for making this known and helping us investigate.

Juoku - March 27, 2024, 4:54 am

Damn that's crazy ?

So a copied / rebranded, outdated crypter thats also backdoored....

That's just low

Hackers - March 27, 2024, 4:57 am

(Mar 27, 2024 04:54 AM)Juoku Wrote: [\[CITE\]](#) Damn that's crazy ?

So a copied / rebranded, outdated crypter thats also backdoored....

That's just low

Yep and [SIM-2362145](#) also made comments about him knowing that I talked to some of his previous customers, but at least 1 told me they never mentioned that to him - pretty sure they were ratted and he was able to see their HF convo w/ me.

also lets not forget that even though [SIM-2362145](#) is distributing copies of ByteProtector V3 in his ByteCrypter sales thread, he simultaneously claims to have never heard of Byte Protector. Just more evidence of his manipulation and lies.

Komodo - March 27, 2024, 5:10 am

Idk shit about this topic but honestly just wanted to say you're super smart.

I enjoy reading your posts about how things work and when you bring people into the spotlight for being shady.

Thanks for protecting the community.

Hackers - March 27, 2024, 5:39 am

(Mar 27, 2024 04:50 AM)Scrubspooof Wrote: [\[CITE\]](#) Hasn't this guy been closed like 5 times now? AFAIK, [SIM-2362145](#) is just a "proxy seller" and it has always been said that he is not the same user [Royal !](#) ...although I think it is, some people claim that Royal's bytecrypter was always 0 FUD but that SIM can barely get below 20. So, it's possible they are two different users, but it's very clear to me that SIM's version is infected, hasn't been updated, etc. If they aren't the same user, then I'm assuming SIM probably doesn't have source at all and is just re-selling the same compiled program. This would also explain why he can't get FUD and why there are so many tools that must be used for 1 crypt.

(Mar 27, 2024 04:52 AM)Euaggelistes Wrote: [\[CITE\]](#) Thank you so much for making this known and helping us investigate.

You're welcome ~ I hope others will help identify scammers too.

(Mar 27, 2024 05:10 AM)Komodo Wrote: [\[CITE\]](#) Idk shit about this topic but honestly just wanted to say you're super smart.

I enjoy reading your posts about how things work and when you bring people into the spotlight for being shady.

Thanks for protecting the community.

Thanks, I appreciate that. I think a lot of this stuff can be found by anyone that wants to try, it didn't take much effort to discover all this, but it did take up a lot of time initially.

Kompers - March 27, 2024, 2:59 pm

Pretty wild. Thanks for posting this.

Scrubspooof - March 27, 2024, 4:02 pm

I never understood why someone would backdoor a product that is already a turn key operation.

Omniscient - March 29, 2024, 11:29 am

Please note that [Hackers](#) did not get the file directly from the seller but instead used a 3rd party to obtain it. This leaves room for doubt. He's also expressed interest in creating his own product/service to compete.

I'm all for protecting the community but I'm also not going to allow a member to harass sellers continually.

[Hackers](#) will be closed if this continues.

