

Forum:[Hack Forums](#)

Thread: [AES and RSA enough for silent miner?](#)

raymundo - October 3, 2023, 3:00 am

I am weary about using a public crypter for detection and AV database reasons, I know how to encrypt files but only on a basic level.

Would generating an AES key and using it to encrypt the data, then generating an RSA key pair and use the RSA public key to encrypt the AES key be enough to avoid detection for a silent miner on WD10, 11, and mcafee be enough? I'm not too privy to triple DES and other encryption algorithms.

If not, can anyone point me in the direction of a good crypter? I'm paranoid about using PureCrypt because so many people use it and i'm sure AV detection is getting used to it, because I really don't want to load hundreds of bots and then have half of them end up detecting my miner.

Ph4n70M Phr34K - October 3, 2023, 3:16 am

(Oct 3, 2023 03:00 AM)raymundo Wrote: [\[CITE\]](#) I really don't want to load hundreds of bots and then have half of them end up detecting my miner.

And you should be aware that you will not avoid that no matter what.

You basically described running a botnet in a nutshell.

You load bots and you lose them. Thats common thing. With time you can learn how to hold them a bit longer, but with silent mining there is not much you could do.

raymundo - October 3, 2023, 3:22 am

(Oct 3, 2023 03:16 AM)Ph4n70M Phr34K Wrote: [\[CITE\]](#) And you should be aware that you will not avoid that no matter what.

You basically described running a botnet in a nutshell.

You load bots and you lose them. Thats common thing. With time you can learn how to hold them a bit longer, but with silent mining there is not much you could do.

So either way, publicly available crypt vs my own crypt it wouldn't make a noticeable difference in longterm runtime?

Ph4n70M Phr34K - October 3, 2023, 3:32 am

(Oct 3, 2023 03:22 AM)raymundo Wrote: [\[CITE\]](#) So either way, publicly available crypt vs my own crypt it wouldn't make a noticeable difference in longterm runtime?

It would make a noticeable difference for sure.

But you still need to be aware that running a botnet is a constant work with monitoring and maintaining and you will be always losing bots, no matter what.

Night Storm - October 3, 2023, 5:37 am

(Oct 3, 2023 03:22 AM)raymundo Wrote: [\[CITE\]](#) So either way, publicly available crypt vs my own crypt it wouldn't make a noticeable difference in longterm runtime?

Public Crypter signatures are already in circulation, Thus = Lots of detection.

Private Crypter = It is not about AES encryption only that makes your stub FUD. If it was that easy you would've seen lots of crypter in the market. AVs detect your stub based on the common method that you can use to encrypt. Trying to double triple encryption will certainly lead to corrupt stub than

a working one.

TIP: Not sure which programming language you are using to build it but, for me a crypter coded in C++ is much easier to make your stub FUD. Also, try to inject in process memory and hide it from task manager list. If possible, you can also try to bind it with system process. This ensures persistence and long time FUD of your stub.

PureCoder - October 3, 2023, 12:23 pm

(Oct 3, 2023 03:00 AM)raymundo Wrote: [\[CITE\]](#) Would generating an AES key and using it to encrypt the data, then generating an RSA key pair and use the RSA public key to encrypt the AES key be enough to avoid detection

AES key has nothing to do with FUD. Actually this method (AES + RSA) is used by r*nsomware for encrypting files, not for crypters.

You can just use AES or TripleDES.

raymundo - October 3, 2023, 11:00 pm

(Oct 3, 2023 12:23 PM)PureCoder Wrote: [\[CITE\]](#) AES key has nothing to do with FUD. Actually this method (AES + RSA) is used by r*nsomware for encrypting files, not for crypters.

You can just use AES or TripleDES.

Thank you for the reply, very helpful. Does the crypter you sell have UAC bypass? I've been looking into PureCrypter recently.

(Oct 3, 2023 03:32 AM)Ph4n70M Phr34K Wrote: [\[CITE\]](#) It would make a noticeable difference for sure.

But you still need to be aware that running a botnet is a constant work with monitoring and maintaining and you will be always losing bots, no matter what.

That's fine though, I would estimate a loss of anywhere between 30-40% of bots per 100, given all factors.

DramaKing - October 5, 2023, 7:36 pm

A simple encryption of your miner will not bypass runtime detection. AV and AMSI will simulate the execution, test what the unencrypted code does, and quarantine it.