

Forum:[Hack Forums](#)

Thread: [UnamSanctam Miner Crypter](#)

whoisthisss - May 31, 2023, 4:46 am

hi, i need a crypter to encrypt the miner of unam sanctam can experienced people give me some advice what should i buy?

malik257 - August 6, 2023, 4:55 am

I'd like to know what's best for this aswell as have been looking for a while

osn64698 - August 6, 2023, 5:03 am

You can't make malware like that fully runtime FUD.

SIM-5084802 - August 7, 2023, 7:14 am

(May 31, 2023 04:46 AM)whoisthisss Wrote: [\[CITE\]](#) hi, i need a crypter to encrypt the miner of unam sanctam can experienced people give me some advice what should i buy?

(Aug 6, 2023 04:55 AM)malik257 Wrote: [\[CITE\]](#) I'd like to know what's best for this aswell as have been looking for a while

Actually I made it work for myself, fully crypted with 0/26 at avcheck and antiscan too. Bypass windows defender on runtime.

(Aug 6, 2023 05:03 AM)osn64698 Wrote: [\[CITE\]](#) You can't make malware like that fully runtime FUD. Actually yeah you can if you change it just a little and make a good encryption. Not wanting to offend anyone or say anyone is wrong, just talking from my own personal experience.

osn64698 - August 7, 2023, 8:01 am

(Aug 7, 2023 07:14 AM)SIM-5084802 Wrote: [\[CITE\]](#) Actually I made it work for myself, fully crypted with 0/26 at avcheck and antiscan too. Bypass windows defender on runtime.

Actually yeah you can if you change it just a little and make a good encryption. Not wanting to offend anyone or say anyone is wrong, just talking from my own personal experience.

You actually do not know what you are talking about, no offense my man. But saying "0/26" at avcheck and antiscan just proves that fact.

You should differentiate between Scantime / Runtime detection. Defender is not usually a "hard" thing to bypass, it is actually the easiest one.

Go download a free trial of BitDefender / Kaspersky/ MalwareBytes/ ESET or any other AV, and see how your "0/26" becomes "10/26" runtime.

Nobody cares about a scan at "av-check" or "antiscan", only scammers on HF love to show that OFF, what is the point of having scantime FUD to only get detected in the first second your file is opened? How is that even relevant?

It is like flexing that you have "1 million" dollars, but you can't actually use it to buy anything, but hey showing off is important!

Modern AV's have long shifted to Heuristic/ dynamic analysis/ Cloud scanning which is never done scan time, only on file execution. That is why it is so important to break emulators, stall the execution, and use creative ways for each stage of execution. Heck ESET for example employs some good-ass memory scanning, so if your crypter "decrypts" your payload in runtime, it will still get detected, but at a later stage.

AVs generally do not only rely solely on static analysis, they install driver callbacks, those callbacks are called on handle operation, registry, file creation, etc.

So if your "MALWARE" is using (Just for the example) the most trivial way of "startup", it will still show 0/35 in "antiscan" and you can be very happy and flex it to your HF buddies, but it will get detected runtime, and no CRYPTER can help you you change that fact unless you get to the root cause, which is: the malware you use.

That is why it is so important to use proper malware even before starting to think about a "Crypt". A crypt guarantees execution of the original payload, not lifetime.

Even if you pay 10k\$, you can't make Unam FUD runtime, unless you can actually unload all the mechanisms of the antivirus, which I highly doubt people here are capable of.

This is also why as a malware creator you should test your malware against all AVs at each development stage and adapt it per AV, something that flies with 1 AV won't fly with another.

With such attention to detail, you will have 1 month + of FUD time, even if you submit the sample 100 + times to VT. The big shame is that not a lot of people on HF like to use their brains to find creative ways, instead, they prefer to be spoon-fed with outdated methods. Just look at the crypter section.

SIM-5084802 - August 7, 2023, 10:48 am

(Aug 7, 2023 08:01 AM)osn64698 Wrote: [CITE](#) You actually do not know what you are talking about, no offense my man. But saying "0/26" at avcheck and antiscan just proves that fact.

You should differentiate between Scantime / Runtime detection. Defender is not usually a "hard" thing to bypass, it is actually the easiest one.

Go download a free trial of BitDefender / Kaspersky/ MalwareBytes/ ESET or any other AV, and see how your "0/26" becomes "10/26" runtime.

Nobody cares about a scan at "av-check" or "antiscan", only scammers on HF love to show that OFF, what is the point of having scantime FUD to only get detected in the first second your file is opened? How is that even relevant?

It is like flexing that you have "1 million" dollars, but you can't actually use it to buy anything, but hey showing off is important!

Modern AV's have long shifted to Heuristic/ dynamic analysis/ Cloud scanning which is never done scan time, only on file execution. That is why it is so important to break emulators, stall the execution, and use creative ways for each stage of execution. Heck ESET for example employs some good-ass memory scanning, so if your crypter "decrypts" your payload in runtime, it will still get detected, but at a later stage.

AVs generally do not only rely solely on static analysis, they install driver callbacks, those callbacks

are called on handle operation, registry, file creation, etc.

So if your "MALWARE" is using (Just for the example) the most trivial way of "startup", it will still show 0/35 in "antiscan" and you can be very happy and flex it to your HF buddies, but it will get detected runtime, and no CRYPTER can help you you change that fact unless you get to the root cause, which is: the malware you use.

That is why it is so important to use proper malware even before starting to think about a "Crypt". A crypt guarantees execution of the original payload, not lifetime.

Even if you pay 10k\$, you can't make Unam FUD runtime, unless you can actually unload all the mechanisms of the antivirus, which I highly doubt people here are capable of.

This is also why as a malware creator you should test your malware against all AVs at each development stage and adapt it per AV, something that flies with 1 AV won't fly with another.

With such attention to detail, you will have 1 month + of FUD time, even if you submit the sample 100 + times to VT. The big shame is that not a lot of people on HF like to use their brains to find creative ways, instead, they prefer to be spoon-fed with outdated methods. Just look at the crypter section.

Hey, you don't have to get triggered over nothing. I was talking about scantime, but runtime is 2/20 on scanner.to, which is full runtime with internet on.

I am aware of all the facts you handed over here, and if I were you I would stop underestimating what HF community can or cannot do, since you are a part of it LOL. Would be nice if you stated facts more gently and nice, it wouldn't hurt your reputation I am sure.

Sorry if my post offended you, but I was just stating what my past experience was. You don't have to offend people to make your point.

Don't bother answering, I'm out of here... Cheers

osn64698 - August 7, 2023, 11:30 am

(Aug 7, 2023 10:48 AM)SIM-5084802 Wrote: [\[CITE\]](#) Hey, you don't have to get triggered over nothing. I was talking about scantime, but runtime is 2/20 on scanner.to, which is full runtime with internet on.

I am aware of all the facts you handed over here, and if I were you I would stop underestimating what HF community can or cannot do, since you are a part of it LOL. Would be nice if you stated facts more gently and nice, it wouldn't hurt your reputation I am sure.

Sorry if my post offended you, but I was just stating what my past experience was. You don't have to offend people to make your point.

Don't bother answering, I'm out of here... Cheers

You see, this is exactly why it is never worth explaining anything to people here, they simply ignore it and think they are too smart.

Whatever dude, gl with your "FUD" MINER.

Ukamana - August 7, 2023, 3:06 pm

(May 31, 2023 04:46 AM)whoisthiss Wrote: [\[CITE\]](#) hi, i need a crypter to encrypt the miner of unam sanctam can experienced people give me some advice what should i buy?

you can write to my telegram i can help you, because im use too him miner, and i'm coded mini crypter - good 1-2\28 detect

telegram: [deleted] [warn]

Ph4n70M Phr34K - August 8, 2023, 4:25 am

(Aug 7, 2023 11:30 AM)osn64698 Wrote: [\[CITE\]](#) You see, this is exactly why it is never worth explaining anything to people here, they simply ignore it and think they are too smart.

Whatever dude, gl with your "FUD" MINER.

I can understand why you get such impression. But your high quality posts are good for the observers and lurkers that doesn't want to contribute.

It's hard to convince the idiots we usually argue with. In fact its impossible. But the smart people who are reading this will always find something valuable and thats why its worth to contribute.

At least thats my point of view and reasons why i often openly argue with idiots and scammers, even when i know they won't give up.