

Forum:[Hack Forums](#)

Thread: [Private stub detections, problem with gen variant, don't bypass google chrome downloa](#)

Jhonnycash779 - April 20, 2022, 4:33 pm

Hello,

I ran into some different problems with the crypter i have, which i know work for some others.

I'm not a specialist, but i'll try to explain the situation:

So i make a build with async (basic) with no special features, DNS, port etc, then, i test the connection with the unencrypted stub, it works, ok

I log into the crypter, i put my file to crypt, i select the injection corresponding to Async rat (.Net4), no startup, nothing more than that, then i crypt (so it should be less detect because less features integrate in the stub right?)

I scan my file (.exe crypted), into avcheck, or antiscan.me, in best cases, i have 0/26, but it can be 4 or 5/26 in worst cases, which i think is not that bad, as the only av the flash is esetnod, avg and others, no avast, no WD detect.

Then, i try in 'real' conditions, sending the crypted stub by file.io on another VM which is on a different network. I try do download it from google chrome, AV on, no sharing sample of course, and the thing is, sometimes it will not even bypass google chrome download scan, sometimes it will do lol.. (at 0/26 of course in most cases it bypass the browser) (at 1-5/26, it don't even bypass the browser security lets say 80% of the time).

Additionally to that, when the file is being download without problems, there is not only the smart screen that can pop up, but also grey windows of WD security on the bottom right of the screen lol.

Is this shit happen to everybody? What i may be doing wrong?

I want to start a real things, but how do you manage to run campaigns with thoses problems? or maybe i'm the only one lol

Thank you for the time you took to read this, hope someone have already encounter this type of things.

Good day to all

Jhonnycash779 - April 21, 2022, 5:59 am

(Apr 21, 2022 04:39 AM)Dyne Wrote: [\[CITE\]](#) Any .exe that is recently signed, not cross reference downloaded(very important!) from multiple PCs logged without problems or contain generic dormant malicious code will be detected by browser download.

Everything scans and high scrutiny items have their samples delivered. Email scans, browser scans, desktop scans, memory scans... Zoneldentifiers are your worst enemies.

And youre also describing a public or shared stub crypter.
Runtime and scantime are drastically different.
Hello Dyne,

First thanks for your reply,

I'm talking about a private crypt stub.

I started to think that maybe, doind many tests on the same VM, where malicious code where already deliver by the past, could not be the better options maybe?

Is it better to test on new Clean VM each times? to not affects the detections etc?

Look, now my private stub have been updated (today), i'm getting 1/26 detection instead of 5/26, i've tested to deliver the malware thru a .rar protected archive, so it bypass chrome detection successfully, BUT, once i extract the content of the archive in the victim computer, and try to launch the .exe, a pop up error from windows says, impossible to open the file, a virus is detected, BUT I have 0/26 detection lol, and i can't find any runtime scanner here.

I don't understand how you guys manage to run campaign all over the year with that types of problematic, which, i believe, you must not encounter LOL

Jhonnycash779 - April 21, 2022, 9:57 am

(Apr 21, 2022 09:32 AM)Dyne Wrote: [\[CITE\]](#) Scantime and runtime are different.

The only proper Runtime check scanner is dyncheck, which is paid and more expensive for realtime format with internet connection.

Manually checking with virtual machines is always an option as well. Eset licenses are pretty cheap, just make sure nothing submits a sample and roll back your snapshot.

But what youve described is scantime packed FUD, not runtime.

Good luck!

Yes sure i understand the difference,

Unfortunately, i'm unable to access dyncheck.com.. as i think it goes mia since few months

Thank you for your time

GiraffeBear - April 21, 2022, 11:27 am

(Apr 21, 2022 09:57 AM)Jhonnycash779 Wrote: [\[CITE\]](#) Yes sure i understand the difference,

Unfortunately, i'm unable to access dyncheck.com.. as i think it goes mia since few months

Thank you for your time

I think you can try Checkzilla as well.

Jhonnycash779 - April 21, 2022, 3:04 pm

(Apr 21, 2022 11:27 AM)GiraffeBear Wrote: [\[CITE\]](#) I think you can try Checkzilla as well.

thanks you for your answer i'll check that

nothing0x0 - May 9, 2022, 11:59 am

(Apr 20, 2022 04:33 PM)Jhonnycash779 Wrote: [\[CITE\]](#) Hello,

I ran into some different problems with the crypter i have, which i know work for some others.

I'm not a specialist, but i'll try to explain the situation:

So i make a build with async (basic) with no special features, DNS, port etc, then, i test the connection with the unencrypted stub, it works, ok

I log into the crypter, i put my file to crypt, i select the injection corresponding to Async rat (.Net4), no startup, nothing more than that, then i crypt (so it should be less detect because less features integrate in the stub right?)

I scan my file (.exe crypted), into avcheck, or antiscan.me, in best cases, i have 0/26, but it can be 4 or 5/26 in worst cases, which i think is not that bad, as the only av the flash is esetnod, avg and others, no avast, no WD detect.

Then, i try in 'real' conditions, sending the crypted stub by file.io on another VM which is on a different network. I try do download it from google chrome, AV on, no sharing sample of course, and the thing is, sometimes it will not even bypass google chrome download scan, sometimes it will do lol.. (at 0/26 of course in most cases it bypass the browser) (at 1-5/26, it don't even bypass the browser security lets say 80% of the time).

Additionally to that, when the file is being download without problems, there is not only the smart screen that can pop up, but also grey windows of WD security on the bottom right of the screen lol.

Is this shit happen to everybody? What i may be doing wrong?

I want to start a real things, but how do you manage to run campaigns with thoses problems? or maybe i'm the only one lol

Thank you for the time you took to read this, hope someone have already encounter this type of things.

Good day to all

Any .exe file is detected, no matter scantime-runtime fud, without digital signature, it's almost impossible. even if you pass, you'll see your wacatac soon.

Jhonnycash779 - May 9, 2022, 12:36 pm

(May 9, 2022 11:59 AM)nothing0x0 Wrote: [\[CITE\]](#) Any .exe file is detected, no matter scantime-runtime fud, without digital signature, it's almost impossible. even if you pass, you'll see your wacatac soon.

do you think getting a great .lnk exploit and putting the malware innit could work better?

mkdiretc - April 28, 2023, 2:48 am

Yes, we need solutions. I will share if I find something usefull.

3cho\$trike - May 1, 2023, 11:39 am

Are you using free or paid dns ? I used noip and private stub and got detections after 2-4 days of using.

Just learn it now :) try it - might help :) pm me if you have questions