

Forum:[Hack Forums](#)

Thread: [Google Chrome detects Virus](#)

scoopyy - May 12, 2022, 6:39 am

Hello everyone,

I've got a fairly simple question.

I'm using asynchrat as part of my investigation in the hacker-world.

But when I build the .EXE and compress it with .RAR it's still detectable by chrome?

Is there any way around this?

As I don't want people to see it's a virus of course.

Thanks a lot! ?

scoopyy - May 12, 2022, 6:53 am

(May 12, 2022 06:49 AM)Dyne Wrote: [\[CITE\]](#) Are you being serious my guy?

Are you putting a password on it?

Many, many people do this; thereby most browsers detect RAR with just an .exe file inside as a potential virus.

Encryption and cryptography will be your best friend. The days of sending a raw .exe by email or by any other channel are long gone, they often must be called from host and executed via Download&execute task.

Malware is not often spread successfully by direct spreading a RAT. Successful actors spread a loader without behavioral runtime detections, and D&E their tool after successful management of their AV.

Hey Dyne,

Yes, I was being serious. I'm new to this and I'm trying to figure everything out and learn from the forum. Sorry for not understanding that something like this is dumb to ask.

Thanks again though for your reply and explaining it a little bit. ?

scoopyy - May 12, 2022, 7:04 am

(May 12, 2022 06:55 AM)Dyne Wrote: [\[CITE\]](#) Hey, not what I meant my guy,

Sorry if that came off as "matter-of-fact" and arrogant.

Best of luck!

Common delivery methods are .lnk, .xlsm, .vba which execute a download&execute of your loader/botnet stub. (In cheaper malware, often done solely by powershell script)

Damn, I didn't even think about that. So you can use .lnk to run a script? And is the loader/stub part of the build .EXE file or don't you even need the EXE file if you already have a loader/stub on the target's computer?

Thanks again for replying and no worries about your comment. ?

scoopyy - May 12, 2022, 7:24 am

(May 12, 2022 07:21 AM)Dyne Wrote: [\[CITE\]](#) The .lnk, though saturated now, is heavily used as a decoy.

> The botnet stub is hosted on www.yourdomain.com/yourexe.exe encrypted with a private stub crypt.

> The .lnk executes script that downloads first www.yourdomain.com/yourtextorjpgfile.jpg which opens a .jpg on the desktop as a decoy, then silently download and executes your .exe from www.yourdomain.com/yourexe.exe

The .lnk can have its icon changed with a tool like Resource Hacker which places a different .ico file.

ALot goes into delivering a crypted .exe, beyond just clicking a button that says "crypt". Signing, certifying and hosting on an AGED domain with reputable traffic is just the surface.

Hope this helps.

I will side note, you still cannot download a .lnk directly from google chrome or browser because of abuse in the past few years.

Thank you so much for this explanation! I wish I could reward you with a lot of ??, but I'm poor so.

There are few people who really offer information like this so I'm really appreciative.

Grtz,

Scoopyy ?

(May 12, 2022 07:24 AM)scoopyy Wrote: [\[CITE\]](#) Thank you so much for this explanation! I wish I could reward you with a lot of ??, but I'm poor so.

There are few people who really offer information like this so I'm really appreciative.

Grtz,

Scoopyy ?

I just noticed you donated 500 ?, Thank you so much. Now I'm not poor anymore ?.

Is there any way to befriend someone on here or isn't that a thing?

biggioturbomaster - May 17, 2022, 3:02 pm

Write your own crypter and be a cool 1337 hax0r... don't spread malware but instead do it to learn how it works and never commit crimes.

Stay right, stay whitehat.

:wq!