

Forum:[Hack Forums](#)

Thread: [Weird slaves showing up?](#)

Tyler Durden. - January 4, 2017, 9:41 am

Hello

So I am using Imminent Monitor, and Cyberseal Protector.

I just built a new server, and crypted it with CyberSeal protector.

- Now I haven't even spread the file yet, and only after about 5 min after crypting my file, these slaves show up. Now are these HoneyPots, and how the hell did they end up there, when I JUST created the server?

Spoiler ([Click to View](#))

<https://imgur.com/a/MFwwg>

chase. - January 4, 2017, 9:42 am

It's the FBI you're fucked dude see ya in prison

Baitable - January 4, 2017, 9:44 am

Usually from VT scans, I suggest you don't use VT for your scanning purposes.

bzr? - January 4, 2017, 9:46 am

Its a honeypot. Your stub has made its way into the hands of the anti virus companies and they're scanning it.. Just block them and be more careful.

Dankkk - January 4, 2017, 9:48 am

I recommend setting your stub up to melt... aswell if you see a VM on your connections or someone trying to fuck with your stub in a VM or in CMD you should most deffs uninstall the payload. fuck the feds OP ?

President Morty - January 4, 2017, 9:48 am

Its the FBI dude you're fucked, throw your hard drive in a river.

Its a honey pot mostly likely someone scanned your file on VirusTotal.

Tyler Durden. - January 4, 2017, 9:51 am

Listen.

The file never left my computer + the only scanner I used was the inbuilt scanner in CyberSeal. Now I doubt the creator is stupid enough to implement VirusTotal into his own crypter?

Just trying to understand how the honeypots received the file then.

White. - January 4, 2017, 9:53 am

(Jan 4, 2017 10:51 AM)Tyler Durden. Wrote: [\[CITE\]](#) Listen.

The file never left my computer + the only scanner I used was the inbuilt scanner in CyberSeal. Now I doubt the creator is stupid enough to implement VirusTotal into his own crypter?

Just trying to understand how the honeypots received the file then.

Do you with any chance run any anti-virus software yourself that might have taken it and decided to scan?

Dankkk - January 4, 2017, 9:53 am

(Jan 4, 2017 10:51 AM)Tyler Durden. Wrote: [\[CITE\]](#) Listen.

The file never left my computer + the only scanner I used was the inbuilt scanner in CyberSeal. Now I doubt the creator is stupid enough to implement VirusTotal into his own crypter?

Just trying to understand how the honeypots received the file then.
what crypter did you get? is it a shady ass crypter ...

Tyler Durden. - January 4, 2017, 9:56 am

(Jan 4, 2017 10:53 AM)Dankkk Wrote: [\[CITE\]](#) what crypter did you get? is it a shady ass crypter ...
Thank you for replying, but read the thread before you post.
CyberSeal

Sheeple - January 4, 2017, 9:56 am

(Jan 4, 2017 10:51 AM)Tyler Durden. Wrote: [\[CITE\]](#) Listen.

The file never left my computer + the only scanner I used was the inbuilt scanner in CyberSeal. Now I doubt the creator is stupid enough to implement VirusTotal into his own crypter?

Just trying to understand how the honeypots received the file then.
Turn off/uninstall any anti-virus software on your pc. Chances are that shit got sent straight to analysis.
Thanks for ruining the detections

ze-slade - January 4, 2017, 9:56 am

Ignore the idiots saying it's the FBI, the clients are just honeypots, your program must've gotten picked up by an anti virus scanner like VT, did you download your stub from Chrome? If so that'd explain it other possibilities: anti virus scanned and distrubuted or you uploaded it to a bad scan site/file upload site

Tyler Durden. - January 4, 2017, 9:56 am

(Jan 4, 2017 10:53 AM)ThatUnnamedWhiteDude Wrote: [\[CITE\]](#) Do you with any chance run any anti-virus software yourself that might have taken it and decided to scan?

No, I am absolutely certain as I currently have 0 antivirus software installed on that computer.

(Jan 4, 2017 10:56 AM)Sheeple Wrote: [\[CITE\]](#) Turn off/uninstall any anti-virus software on your pc. Chances are that shit got sent straight to analysis.

Thanks for ruining the detections

Yes, and thank you for your useless post. I don't have any antivirus software

ze-slade - January 4, 2017, 9:58 am

(Jan 4, 2017 10:56 AM)Sheeple Wrote: [\[CITE\]](#) Turn off/uninstall any anti-virus software on your pc. Chances are that shit got sent straight to analysis.

Thanks for ruining the detections

He's probably new still, judging by the thread. Don't give him such a hard time, we all make mistakes after all, and I'm sure you made one like this before too. ?

White. - January 4, 2017, 9:59 am

(Jan 4, 2017 10:56 AM)Tyler Durden. Wrote: [\[CITE\]](#) No, I am absolutely certain as I currently have 0 antivirus software installed on that computer.

I would suggest that you check out Windows Defender settings as it enables itself if not turned off by user policy or an alternative AV program (Windows 10).

Also, disable your Windows Firewall.

Furthermore, do not download your stub from a browser even when localhost a browser will upload it and scan it.

Other than this you must've been leaking your file somewhere as I can't think of anything else that happened, but these clients are not the end of the world, just block them and be done with them.

Tyler Durden. - January 4, 2017, 10:02 am

(Jan 4, 2017 10:58 AM)ze-slade Wrote: [\[CITE\]](#) He's probably new still, judging by the thread. Don't give him such a hard time, we all make mistakes after all, and I'm sure you made one like this before too. ?

Thank you for the kind words. And yes, I am fairly new to these tools. But I really haven't uploaded it anywhere nor used any thirdparty scanners.

Hell, even my Windows Defender & Firewall is disabled ?

White. - January 4, 2017, 10:06 am

(Jan 4, 2017 11:02 AM)Tyler Durden. Wrote: [\[CITE\]](#) Thank you for the kind words. And yes, I am fairly new to these tools. But I really haven't uploaded it anywhere nor used any thirdparty scanners.

Hell, even my Windows Defender & Firewall is disabled ?

Then I'd just suggest you block those slaves and move on as it can't be traced back to what actually did happen.

ze-slade - January 4, 2017, 10:21 am

(Jan 4, 2017 11:02 AM)Tyler Durden. Wrote: [\[CITE\]](#) Thank you for the kind words. And yes, I am fairly new to these tools. But I really haven't uploaded it anywhere nor used any thirdparty scanners.

Hell, even my Windows Defender & Firewall is disabled ?

Strange, you shouldn't get any detection unless you did something like that, did you possibly drag the file into your chrome window and it "downloaded"?

bzr? - January 4, 2017, 10:23 am

Even if you yourself haven't uploaded anywhere suspicious, if you have spread the file online it's likely that someone has scanned it themselves.

Purple Kief - January 4, 2017, 11:13 am

(Jan 4, 2017 10:46 AM)BzrK Wrote: [\[CITE\]](#) Its a honeypot. Your stub has made its way into the hands of the anti virus companies and they're scanning it.. Just block them and be more careful.

This is the correct answer.

Maybe you had windows defender running?

It's a honeypot, without a doubt.

warpje - January 4, 2017, 11:15 am

You didn't spread or anything but did you ever used an older stub with the same ports?

Sheeple - January 4, 2017, 11:22 am

Did you untick this

<http://prnt.sc/drin76>