Forum:Hack Forums

Thread: I codded a reverse shell and I got an unknown connections

SIM-2778735 - *January 20, 2022, 7:55 am*

Hi, I codded a simple reverse shell for testing/education purpose.
I opened a port on my internet, upload the file to (filebin-dot-com) and downloaded it to a VPS outside my network.

It worked fine, but after a couple minute after, I got an unknown connections pop up into my server side.

How is that possible ? I didnt send the file to someone.

Two things come into my mind, but since im not experienced with this, I want to confirm with you guys.

1 - Does the site where I uploaded the files (filebin) Run all of the uploaded files into a VM?
2 - Maybe the VPS company transfer and run all file that are into their machine?

I just closed my port to make sure that I wont get reverse engineering. Should I be woried?

Thanks.

Dobby - *January 20, 2022, 11:37 am*

Antivirus sample submission - Honeypots

SIM-2778735 - *January 20, 2022, 1:05 pm*

(Jan 20, 2022 12:37 PM)Dobby Wrote: *[CITE]* Antivirus sample submission - Honeypots
from the website where I upload my file or inside my rented VPS

Perplex - *January 20, 2022, 5:52 pm*

(Jan 20, 2022 02:05 PM)tiberhockey Wrote: *[CITE]* from the website where I upload my file or inside my rented VPS
its very possible that the file sharing site are working with AV.

Why would you not just transfer the file over rdp protocol?
If you dont want to do that, atleast upload the builds in a .rar or .zip folder with a password. To avoid automatic scans and distributions

SIM-2778735 - *January 23, 2022, 7:43 am*

(Jan 20, 2022 06:52 PM)Perplex Wrote: *[CITE]* its very possible that the file sharing site are working with AV.

Why would you not just transfer the file over rdp protocol?
If you dont want to do that, atleast upload the builds in a .rar or .zip folder with a password. To avoid automatic scans and distributions
Thanks!

Eclipse - *January 24, 2022, 10:20 am*

(Jan 20, 2022 08:55 AM)tiberhockey Wrote: [CITE] Hi, I codded a simple reverse shell for testing/education purpose.
I opened a port on my internet, upload the file to (filebin-dot-com) and downloaded it to a VPS outside my network.

It worked fine, but after a couple minute after, I got an unknown connections pop up into my server side.

How is that possible ? I didnt send the file to someone.

Two things come into my mind, but since im not experienced with this, I want to confirm with you guys.

1 - Does the site where I uploaded the files (filebin) Run all of the uploaded files into a VM?
2 - Maybe the VPS company transfer and run all file that are into their machine?

I just closed my port to make sure that I wont get reverse engineering. Should I be woried?

Thanks.
like they say. Av Sample machines that test it and stuff. Or ur VPS company or maybe u uploaded to a disturbution malware scanner. if u did

Joseph Ducreux - *January 24, 2022, 11:18 am*
get a whois record on the IP that connected. that can differentiate between security companies, your vps, some other person (etc)

linkinpork - *January 24, 2022, 12:28 pm*
(Jan 20, 2022 08:55 AM)tiberhockey Wrote: [CITE] Hi, I codded a simple reverse shell for testing/education purpose.
I opened a port on my internet, upload the file to (filebin-dot-com) and downloaded it to a VPS outside my network.

...snip...
I just closed my port to make sure that I wont get reverse engineering. Should I be woried?

Organizations like Shodan (https://www.shodan.io/) and Censys (https://censys.io/) do scans of the entire IPv4 landscape on the daily. They must've tripped your open port and ended up sending false alarm saying somebody connected. Or it may've been just some random skid using nmap.

I experience this a lot when I open a Meterpreter listener on my VPS. Time and again randos would try to connect to me.

If you still remember the IP address, you could search it in https://www.abuseipdb.com/

Cheers!