



Operation Pain

Research on a botnet community

Researched by at0m, sysgerm, and Matze from Cosmodium Cybersecurity

How is the botnet sold?

It all starts from a discord named "Pain"

Once we joined the server we saw advertisements for the botnet also named "Pain"

The people who host these botnets like to keep their botnet IP hidden so that sites that malware tracking websites don't get their botnets shut down.

Our mission was to find the IP and expose it to these sites. But our team found way more than expected.

Operation

Step 1. Scroll through the server chats to see if we can find any information on these owners or botnet administrators.

We found 2 IP's that turned out to be slave servers for the botnet:

- 136.175.29.53
- 178.214.181.11

They have been exploited by having default credentials and open ports to the Internet that it does not need.

Step 2. Go into the voice chat where the seller was sharing their screen and get as much as information as we could. Out of this voice chat we found the following:

1. Phone Number
2. Email Address
3. Name
4. Botnet IP and Port (23.147.226.118:1234)
5. Proof of them using the botnet for malicious purposes

Step 3 try to find their exploits and find the login page.

Luckily enough, an NMAP scan brought back a lot of information on the botnet IP:

PORT STATE SERVICE VERSION

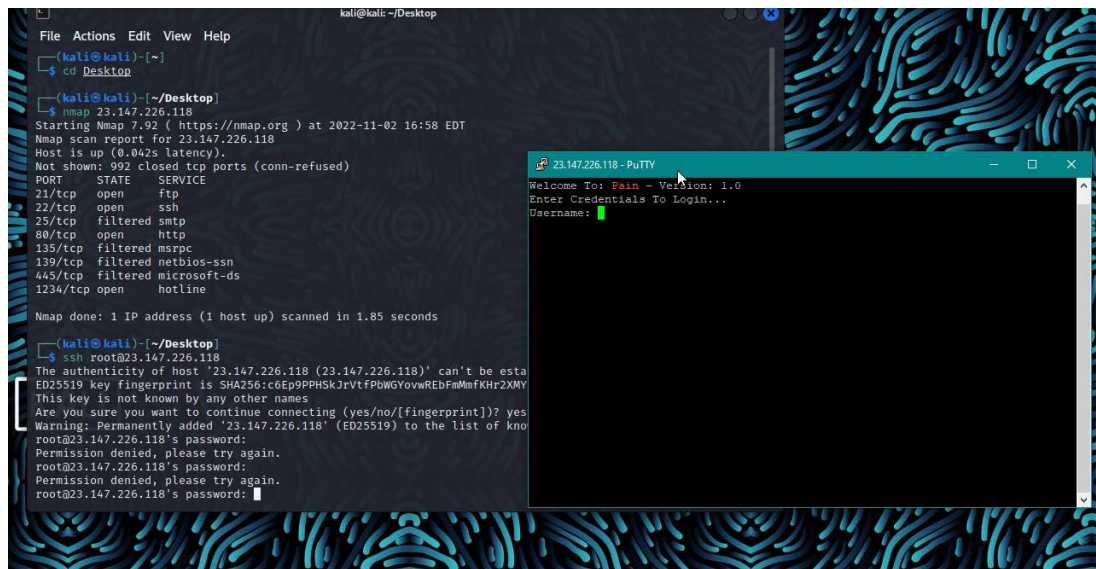
21/tcp open ftp vsftpd 3.0.2

ftp-anon: Anonymous FTP login allowed (FTP code 230)

1234/tcp open hotline?

Port 1234 looked unnormal to have open on a server so we checked it out

once we used PuTTY to connect to the port and IP we were faced with a black page... but my connection was still there. I typed "login" on the blank screen and BOOM!! Botnet login page was found:

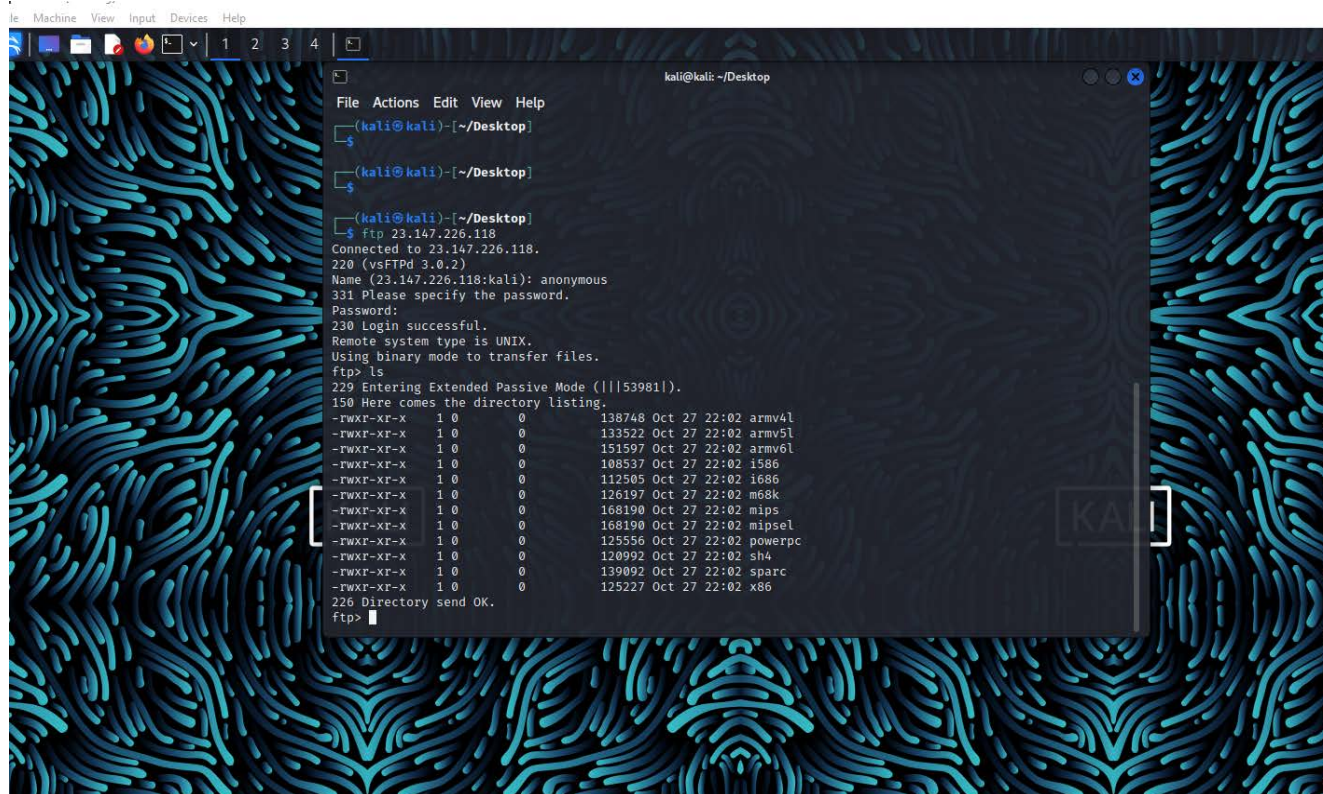


```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~]
$ cd Desktop
(kali@kali)-[~/Desktop]
$ nmap 23.147.226.118
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-02 16:58 EDT
Nmap scan report for 23.147.226.118
Host is up (0.042s latency).
Not shown: 992 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.2
22/tcp    open  ssh
25/tcp    filtered smtp
80/tcp    open  http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1234/tcp  open  hotline
Nmap done: 1 IP address (1 host up) scanned in 1.85 seconds
(kali@kali)-[~/Desktop]
$ ssh root@23.147.226.118
The authenticity of host '23.147.226.118 (23.147.226.118)' can't be established.
ED25519 key fingerprint is SHA256:c6ep9PPH5KJrVtFpUWGyovwREbFmMnFKHr2XMY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '23.147.226.118' (ED25519) to the list of known hosts.
root@23.147.226.118's password:
Permission denied, please try again.
root@23.147.226.118's password:
Permission denied, please try again.
root@23.147.226.118's password:
23.147.226.118 - PuTTY
Welcome To: Pain - Version: 1.0
Enter Credentials To Login...
Username:
```

Next we wanted to look at the FTP server especially because anonymous login was allowed

So, we logged into the FTP server and we found the treasure!!!!

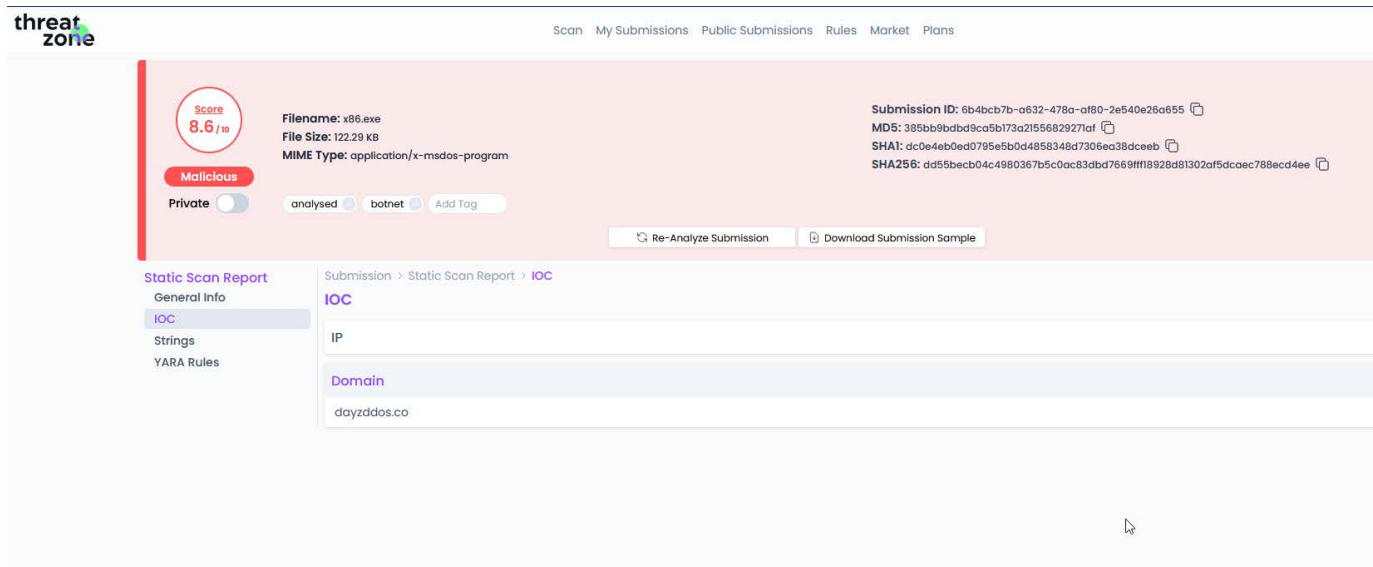
All of the exploits were sitting there waiting for us to analyze:



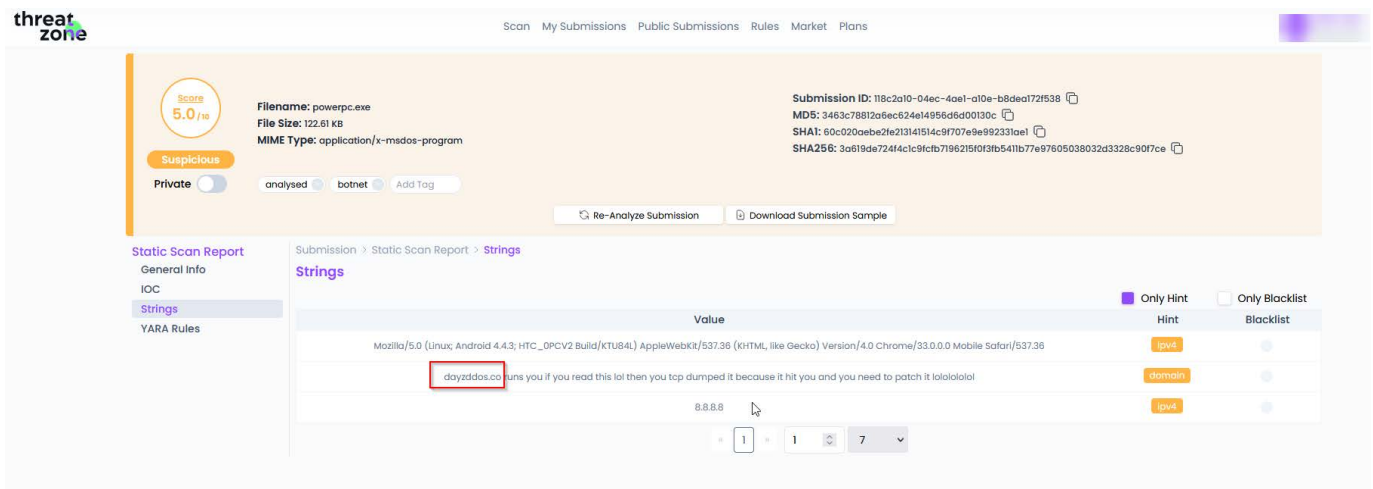
```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$
(kali@kali)-[~/Desktop]
$
(kali@kali)-[~/Desktop]
$ ftp 23.147.226.118
Connected to 23.147.226.118.
220 (vsFTPd 3.0.2)
Name (23.147.226.118:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||53981|).
150 Here comes the directory listing.
-rwxr-xr-x 1 0 0 138748 Oct 27 22:02 armv4l
-rwxr-xr-x 1 0 0 133522 Oct 27 22:02 armv5l
-rwxr-xr-x 1 0 0 151597 Oct 27 22:02 armv6l
-rwxr-xr-x 1 0 0 108537 Oct 27 22:02 i586
-rwxr-xr-x 1 0 0 112505 Oct 27 22:02 i686
-rwxr-xr-x 1 0 0 126197 Oct 27 22:02 m68k
-rwxr-xr-x 1 0 0 168190 Oct 27 22:02 mips
-rwxr-xr-x 1 0 0 168190 Oct 27 22:02 mipsel
-rwxr-xr-x 1 0 0 125556 Oct 27 22:02 powerpc
-rwxr-xr-x 1 0 0 120992 Oct 27 22:02 sh4
-rwxr-xr-x 1 0 0 139092 Oct 27 22:02 sparc
-rwxr-xr-x 1 0 0 125227 Oct 27 22:02 x86
226 Directory send OK.
ftp>
```

Once we had these files it was time to analyze them. So we can share IOCs (Indicators of Compromise) with the community as well as get a better understanding of what these exploits are doing.

We used ThreatZone (threat.zone) and VirusTotal (virustotal.com) to analyze these exploits here are the results and URLs for them:



The screenshot shows the ThreatZone interface for a submission of 'x86.exe'. The score is 8.6/10, labeled as 'Malicious'. The file size is 122.29 KB and the MIME type is 'application/x-msdos-program'. The submission ID is 6b4bcb7b-a632-478a-af80-2e540e26a655. The MD5 is 385bb9bdbd9ca5b173a21556829271af, the SHA1 is dc0e4eb0ed0795e5bd4858348d7306ea38dceeb, and the SHA256 is dd55becb04c4980367b5c0ac83dbd7669fff18928d81302af5dcaec788ecd4ee. The submission is private and has been analyzed, but not yet tagged as a botnet. The static scan report shows the domain 'dayzddos.co' under the 'Domain' section.



The screenshot shows the ThreatZone interface for a submission of 'powerpc.exe'. The score is 5.0/10, labeled as 'Suspicious'. The file size is 122.61 KB and the MIME type is 'application/x-msdos-program'. The submission ID is 118c2a10-04ec-4ae1-a10e-b8dea172f538. The MD5 is 3463c78812a6ec624e14956d6d00130c, the SHA1 is 60c020a6e2fe23141514c9f707e9e92331ae1, and the SHA256 is 3a619de724f4c1c9fcfb7196215f0f3fb5411b77e97605038032d3328c90f7ce. The submission is private and has been analyzed, but not yet tagged as a botnet. The static scan report shows the strings 'Mozilla/5.0 (Linux; Android 4.4.3; HTC_0PCV2 Build/KTU84L) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/33.0.0.0 Mobile Safari/537.36' and 'dayzddos.co runs you if you read this lol then you top dumped it because it hit you and you need to patch it lolololol'. The strings are highlighted in the report.

<https://app.threat.zone/submission/118c2a10-04ec-4ae1-a10e-b8dea172f538/static/>

<https://app.threat.zone/submission/6b4bcb7b-a632-478a-af80-2e540e26a655/static/>

<https://urlscan.io/result/fbf32c75-a072-475c-8265-80c0df5c0ba9/>

<https://www.virustotal.com/gui/file/dc2f933d97cb81d03652dab264aeea7c12a0c6557fe2ff5f3f479a99e9a96b44>

<https://www.virustotal.com/gui/file/36ccd545c1e0b9e32f3f83e5284fbdacbcd43f2070b3e2cd93b04ad07c98a11a>

<https://www.virustotal.com/gui/file/3a619de724f4c1c9fcfb7196215f0f3fb5411b77e97605038032d3328c90f7ce>

IOCs (Indicators Of Compromise):

3463c78812a6ec624e14956d6d00130c

385bb9bdbd9ca5b173a21556829271af

d37d4b6d2c6bd8f128e846ec3f05047a

46ee8b5d1b567628dd0ff9337e674668

ww1[.]dayzddos[.]co

Here is some proof of them using this botnet for malicious purposes:

