Group 1

Mirai Botnet: Security Investments - DRAFT

Rômy Bergman 4369408, Saskia Kooijman 4473795
Jochem van de Laarschot 4227530, Giulio Pellizzari 5143160

30-09-2019

TU Delft
Delft University of Technology

1. *Who is the problem owner of the security issue as measured in your first assignment? (0.5 points)*

The problem owners of the issue of the growth of a Mirai botnet through IoT-devices are the ISPs. ISPs are responsible to maintain the network infrastructure and provide end users access to Internet. Thereby, ISPs possess data about devices accessing the network, such as the source IP address and ports used to route the internet traffic. Therefore, ISPs have a good position in the network to mitigate the growth of such a botnet.
However, the ISPs do not necessarily have an incentive to mitigate the growth of a botnet, since there is no direct impact for the ISP when a botnet grows. Therefore, they need to be incentivized by other actors to use their key position in the network in order to mitigate the growth of a botnet.

2. What relevant differences in security performance does your metric reveal? Evaluate these differences as shown with the metrics developed in the 1st assignment. (2 points)

Two metrics have been defined to mitigate IoT botnets. These are:

- Infection rate: percentage of infected devices relative to the total number of devices for each country per month
- The behavior of Mirai botnets: port distribution over time

Both metrics provide some information about the security performance of ISPs in different countries. In the process of deriving at the conclusions, some assumptions were made which should be noted:

1. To compensate for metric issues regarding multiple IP addresses, the count of IP addresses per day per country was averaged over a month.
2. Each country represents one ISP since we have no data to map each IP address to the ISP it belongs to

The line graphs for the first metric show the 10 worst performing countries (figure 1a) and the best performing countries (figure 1b) in relation to the percentage of infected devices. Figure 1a contains countries with a generally lower GDP than countries in figure 1b (see table 1). This indicates that countries with a lower GDP perform worse than countries with a high GDP. The countries shown in figure ab might have a smaller budget to implement risk strategies and therefore require specific recommendations to create high impact for minimal costs.

[insert table GDP per country: https://www.worldometers.info/gdp/gdp-by-country/]

Percentage of infected devices per month per country

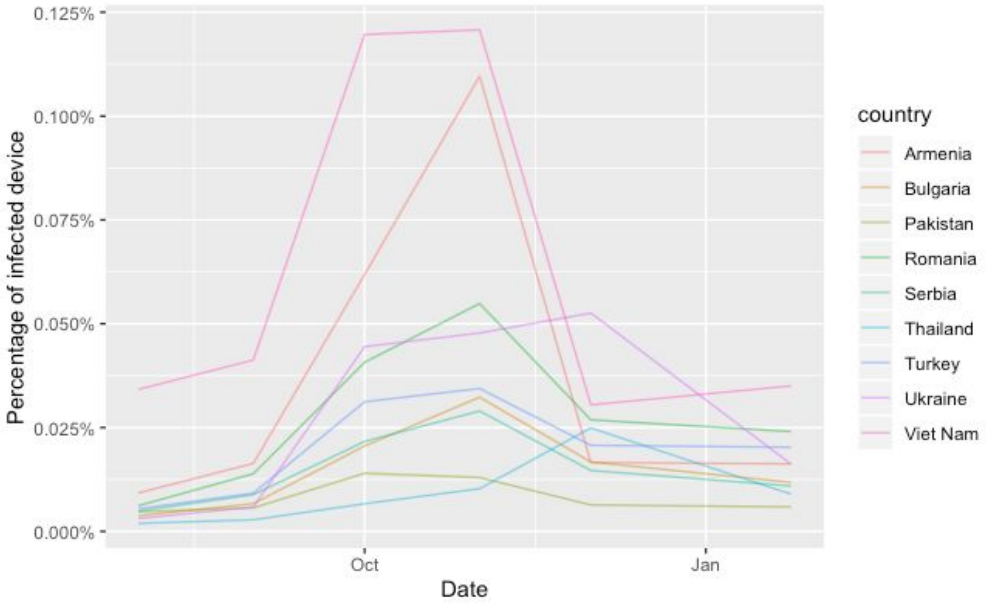

Figure 1a: line graph size of infected devices 10 worst performing countries

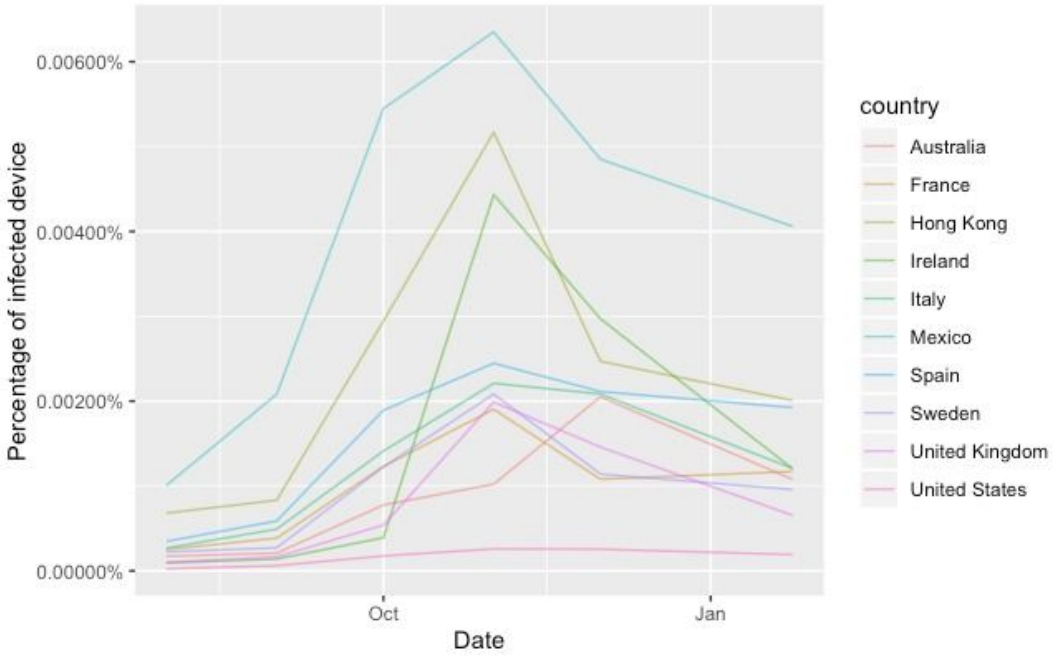

Figure 1b: line graph size of infected devices 10 best performing countries

Finally, the behavior of Mirai botnets shows which ports are scanned by the malware. The port distribution can also be composed per country. Consequently, the scanned ports represent different protocols and traffic. Hence, ISPs in different countries can be advised about which ports should be better protected. For example, port 23 could be primarily scanned in Vietnam and port 5555 in Germany. Besides, the port distribution indicates what devices are the focus of attack because different types of ports can be used to infected different types of IoT-devices.

This offers ISPs the knowledge of which IoT devices are extra vulnerable. Therefore, ISPs can implement strategies more directed to protecting a specific category of IoT devices.

3. What risk strategies can the problem owner follow to reduce the security issue as measured in your first assignment? (0.5 point)

ISPs have three kinds of categories to reduce the growth of a Mirai botnet. These are avoiding, mitigating, accepting and transferring. Question: Should we discuss *possible* cyber insurance schemes for risk transfer strategies?

First of all, the ISPs can avoid the risk of a growing botnet by blocking specific ports. Even though this is a possible strategy, it is not desirable to block a port. When ports are blocked, multiple services cannot be performed. Therefore, this strategy will reduce the ISP's operability. But for the purpose of specifically mitigating the growth of a Mirai botnet, blocking ports is a possible strategy.

Secondly, the security issue can be mitigated. An example of mitigation strategies is awareness campaigns. ISPs can inform the users about the risk of not changing the default password. This creates awareness about the importance to change default passwords as soon as possible. Besides, clear instructions can be provided to IoT device users about how to clear their IoT device from the Mirai virus. This way, users can clean their own device as quickly as possible from the Mirai virus. Another mitigation strategy can be to use intrusion detection systems and intrusion prevention systems. These systems scan the traffic over the network and find out what traffic does not comply with their policy. The detection systems can only detect what traffic does not match their policy but the prevention system also blocks this traffic from going further. Detection prevention systems use *fingerprinting*. A monitoring device recognizes the binary file of the Mirai malware and prevents the IoT device from downloading the file.

Third, the risk can be accepted. If the percentage of IoT devices that carry the Mirai virus is below a certain threshold, the existence of the botnet could be accepted. Only when this percentage is higher than the threshold, the risk of a botnet is increasing and the risk cannot longer be accepted. This threshold will be determined by the ISPs.

4. What other actors can influence the security issue as measured in your first assignment? (1 point)

Governments

Governments are in the position to issue specific laws to prosecute cyber-crime.This is most effective when it's consistent and coordinated between countries (Silva, Silva, Pinto, Salles 2012). When a comprehensive legal framework is in place, this could be a risk mitigation strategy in the following ways:

1. By assigning liabilities, security externalities can be internalized (van Eeten & Bauer, 2009). When actors are held accountable for their poor security, rational actors would invest more in their security practices, reducing the spread of Mirai.
2. People would refrain from becoming a botnet *master* when it's more likely that they get tracked down. This avoids Mirai spreading.

Not only through thorough prosecution governments can push other actors towards more security. Also through other measures governments can pressurize or incentivize other actors (including ISPs, end-users and IoT vendors) to fix their insecure practices (Jerkins, 2017). By incentivizing these actors, the problem is tackled at it source. IoT manufacturers are pressured not to use default credentials, end-users are made more aware and ISPs secure their network: this also mitigates the risk of Mirai spreading.

Depending on the in assignment 1 developed metric *infection rate* which denotes the amount of infected IoT generated traffic relative to the total number of IoT traffic per country, governments may have a certain acceptance strategy as well. When the infection rate is low, government intervention is not deemed necessary and disproportionately expensive.When the issue becomes more pressing and excesses the acceptance threshold, the different mitigation strategies as outlined above can be deployed.

End-users
End-users may not know how to harden the security of their devices. (Silva, Silva, Pinto, Salles 2012). Especially regarding IoT devices, refined permission control is often not feasible due to limited interactions with the device (Bertino & Islam, 2017). The authors note that prevention is the best form of defense and that user awareness is critical since botnet malware mostly spreads through users' mistakes. In terms of risk strategies, end-users should inform themselves and change passwords frequently as a mitigation strategy.

Script kiddies or 'crackers'
As per de Bruijn, Ganan & Van Eeten (2017) crackers, or script kiddies, particularly use botnets to issue DDoS attacks because of their accessibility and easiness in use and their potentially destructive nature. Regarding the security issue, the spread of the Mirai, this group is very influential because the data shows how different versions of the malware developed after the release of the source code. These crackers increase the risk of Mirai becoming more advanced. Since risk strategies for adversaries are deemed out of scope in this paper, it's not further elaborated on how attackers should deal with the risk of being blocked, tracked or obstructed in any other way.

IoT manufacturers
As Kolias, Kambourakis, Stavrou & Voas (2017) argue, IoT vendors have been selling IoT devices with poor security practices. When IoT devices are not shipped with default passwords and provide sufficient security information to the end-users, botnets such as Mirai will not be able to spread using a dictionary attack. These are forms of risk mitigation strategies for IoT manufacturers.

5. (5 points) Pick one of the risk strategies identified previously and calculate the Return on Security Investment (ROSI) for that particular strategy. I.e.,

- Estimate the costs involved in following that strategy
- Estimate the benefits of following that strategy (assume a particular loss distribution)

You must use the dataset to calculate the ROSI and it must include the uncertainty of both the costs and benefits and also be projected in time.

We assume that our strategy is going to decrease the number of infected devices. We also assume that, as consequence of the decrease of the number of bots, the likelihood of a successful DoS causing a complete service unavailability will decrease. Moreover, since we have no information about the source of DoS, for our calculation we assume that all attacks have been generated by an IoT botnet.

Starting from these assumptions, we have used the data provided by Kaspersky to perform the calculation of ROSI and Imperva.
(https://www.kaspersky.com/about/press-releases/2015_collateral-damage-26-of-ddos-attacks-lead-to-data-loss)
(https://www.imperva.com/blog/ddos-impact-cost-of-ddos-attack/).

Among all sectors targeted by DoS attacks reported in Kaspersky report, we consider ISPs can belong to the *Telecommunications* and *IT/software/communication/etc*. We summed the two percentage obtaining 45%: we assume it is the percentage of DoS attack targeting ISPs.

From Kaspersky report we also noticed that 24% of the DoS attacks cause the unavailability of the service. Combining this information with the previous one we get that 11% of DoS causes service unavailability to an ISP.

The Kaspersky report also provides us some data about the duration of the unavailability of the services. Assuming the cost per each hour of unavailability is 40K$ (Imperva) we have the impacts reported in table 1. For each impact the report also provides the percentage of DoS that causes that impact.

Duration (worst case scenario)	% DoS causing unavailability	Impact (K$)
< 10 minutes	10%	7
10 min to 1h	21%	40 (considered 1h)
Several hours	35%	240 (considered 6h)
1 day	14%	960

2 days to 1 week	9%	1.920 (considered 2 day)
Several weeks	7%	6.720 (considered 1 week)

Table 1

From this table, we mapped each duration to the scenario we are studying, the service unavailability of ISPs, as follows:

(1) $P(Duration = X \ \& \ DoS\_to\_ISP) = P(Duration = X) * P(DoS\_to\_ISP)$

Given that $P(DoS\_to\_ISP)$ is 11% we get the result reported in table 2.

Duration (worst case scenario)	$P(Duration = X \ \& \ DoS\_to\_ISP)$
< 10 minutes	1.08%
10 min to 1h	2.27%
Several hours	3.78%
1 day	1.51%
2 days to 1 week	0.97%
Several weeks	0.76%

Table 2

The impact we calculated, showed in Figure 2, shows an estimated average annual loss of 95.800$.

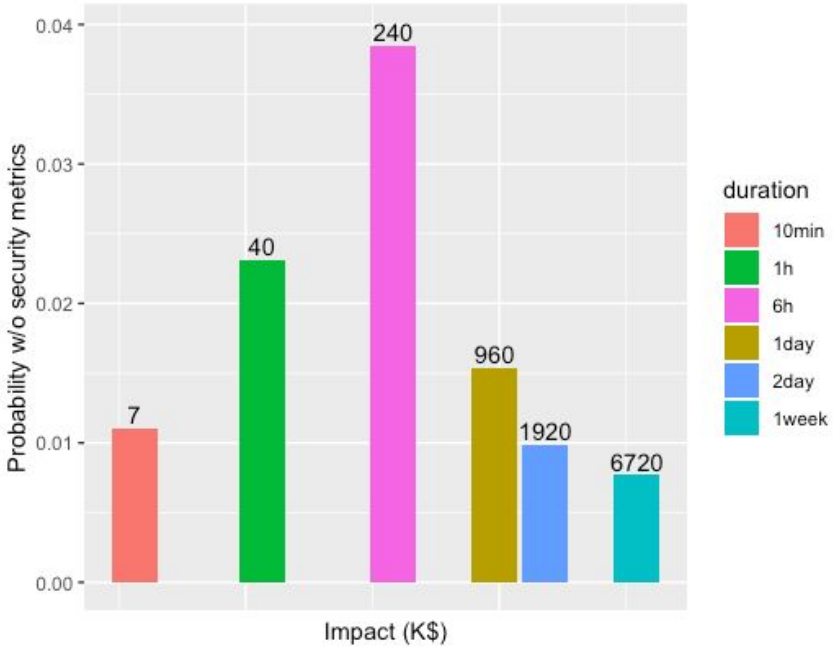

Figure 2

DRAFT - DRAFT - DRAFT - DRAFT - DRAFT - DRAFT - DRAFT - DRAFT - DRAFT - DRAFT

Thanks to the security measure we are going to implement (not yet defined) we are going to decrease the likelihood of a DoS causing unavailability of the service from the actual 24% to 15% (random for now). Thanks to this, we decrease the likelihood computed in (1) to 2% obtaining the result showed in figure 3.

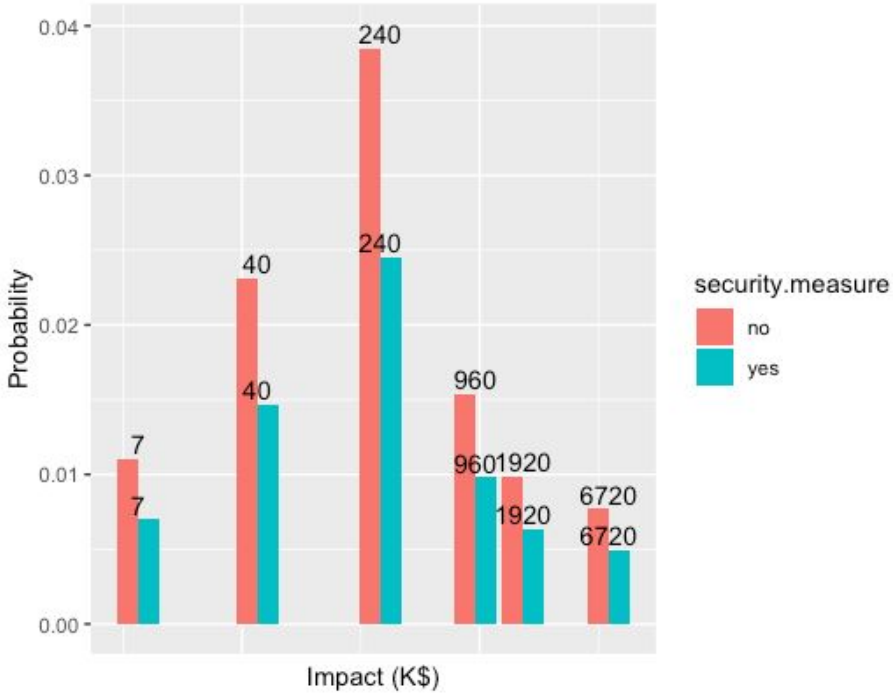

Figure 3

Computing the average annual loss for the solution implementing the security measure we get an expected loss of 61000$.
Since the cost for the implementation of our security metric is 50000$ (random) we compute the ROSI for our solution as:

$$ROSI = \frac{(96800 - 61000) - 50000}{50000} = 6,16$$