Factors impacting botnet infections

By Matthijs Bijman, Max Pigmans, Daniël Vos, Rens Heddes

Introduction

The rise of the Internet of Things (IoT) has lead to widespread use of cheap, poorly secured devices. The volume of and lack of security present in these devices has made them a common vehicle for distributed denial of service (DDoS) attacks performed by botnets. In recent years, several high profile DDoS attacks originated from the Mirai IoT botnet. Since these botnets are mostly used for DDoS attacks or sending spam/phishing emails[1], the owners of these devices do not bear the damages and thus have low incentives to secure their devices[2]. Consequently, most mitigation strategies against botnet attacks are designed for the victims of such attacks[3][4].

In this report we select three actors related to this security issue, analyze how each actor is able to mitigate the risk, how they benefit from this mitigation, but also how others are affected. We then further analyse the performance of all ISPs in a country which is represented by the dataset. To do this, we identify various factors that may explain the variance in the dataset, collect data for these factors, and perform statistical analysis.

Chosen Actors

In this section, we will consider the security issue from the perspective of three related actors. For each of these actors, we identify one concrete countermeasure they could use to mitigate the issue. For each of these countermeasures we then discuss the distribution of costs and benefits among all actors. Based on these costs and benefits we can then analyze whether the actor is incentivized to take the countermeasure. Finally, we will reflect on the role of externalities around the will consider the following three actors:

1. Internet Service Providers. They are the problem owner, and the same factors that made them problem owner in our previous assignment, where we discussed how ISPs are in a good position to see if and how many new devices are being infected and they have the knowledge required to take action against growing botnets. These reasons make them well suited to analyse in this report.
2. Device owners are at the core of the security issue, since their devices are the ones being infected causing the negative externalities for other parties. Therefore device owners have a large impact on the botnet security issue, and have a wide variety of options available to act on it**.**
3. DDoS Victims. Since DDoS victims bear most of the cost of the security issue, we consider it interesting to look at the issue from their perspective and see what countermeasures are available for them.

ISPs

ISPs can mitigate the issue in several ways. By notifying owners of infected devices, by implementing a package filter to stop infections from spreading, and by updating their routers supplied to the customers to prevent them from being infected.

The cost for the ISP to implement a mitigation is relatively high while the benefits are limited. The primary loss associated with the Mirai botnet is unavailability due to a DDoS attack, however in this context the ISP purely is a medium to carry out the attack and not the direct target. This reduces the loss associated with having infected devices in their network to such a degree that ISP’s do not have a direct loss-driven incentive to mitigate the risk.

If the service provider were to mitigate the risk of botnet infections by implementing one or multiple of the aforementioned mitigation tactics, then it would have a positive effect for victims of DDoS attack carried out by the botnet since there will be fewer participating devices and thus a less powerful DDoS attack.

Device Owners

Device owners can mitigate the issue by updating their Internet of Things (IoT) devices and make sure default authentication credentials from the manufacturer are changed to a more secure set of credentials.

The cost for implementing these mitigation strategies is quite low for device owners, since it only requires a small amount of manual work. The benefits, however, are also limited for the device owners, since the devices are primarily used for DDoS attacks which are of little influence to the owners. Therefore, the owners of IoT devices have little incentive to mitigate the risks of the botnet security issues.

In the case that owners of IoT devices should choose to mitigate against having infected devices, then the victims of the DDoS attacks executed by the botnet are positively impacted by having to protect against a smaller attack.

DDoS Victims

The last actor, DDoS victims, can mitigate the issue by investing in a DDoS protection service, which monitors incoming traffic to filter out attacks and they could upgrade server hardware and software to work efficiently under load.

The cost for these solutions is quite high, and in the case of DDoS protection recurring, however the potential losses prevented can easily outweigh the cost for a victim which heavily relies on the availability of their service. Therefore, these actors do have a good incentive to invest in mitigating against potential DDoS attacks.

Implementing these mitigation solutions could have a negative impact on other potential victims, because attackers might choose to target other potential victims with less protection against a DDoS attack.

Actor in Security Metric

To compare countries' security performance regarding the Mirai botnet we looked at how many new IPs were infected in one week per country (the week from 2018-6-1 until 2018-6-7). We chose to look at only one week because the effects of old infected devices having their IP rotated will be less severe. We combine all ISPs in a country because for this aggregation of actors we can a) analyse their performance from the dataset and b) find additional data that may explain the performance. For individual ISPs finding data explaining their performance is infeasible. We assume that ISPs in the same country will have similar policies since they are held to the same regulatory requirements.

We believe the following factors might influence the amount of new infections in a week per country:

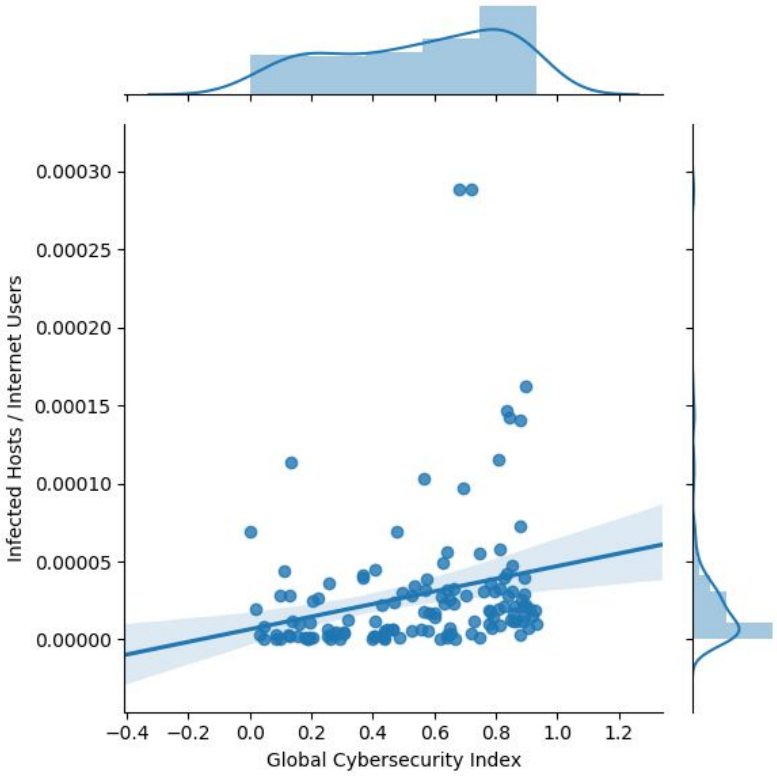
- The country's overall cyber security performance, if a country performs worse overall it might also perform worse in having devices infected by Mirai.
- The country's GDP per capita, a country in which the population does not have much money to spend will likely have fewer electronic devices to be infected per person.
- The country's ICT development level, as more ICT infrastructure might open up the possibility of having more devices infected.

In the rest of this section we collect data on the factors mentioned above and correlate these datasets with the Mirai infected IPs security metric to investigate whether these factors could be used to explain the security performance.

Overall security performance

To measure a country's overall security performance, we make use of 2018's Global Cybersecurity Index (GCI)[1]**.** This index assigns a number between 0 and 1 to each country representing their cyber security performance. The GCI considers five distinct aspects: legal, technical, organizational, capacity building and cooperation. The legal pillar focuses on cybercrime legislation and cybersecurity regulations. The technical pillar looks at, among other things, the implementation of standards, technical measures in place and mechanisms to protect children online. The organizational pillar considers nationwide strategy and responsible central agency. The capacity pillar looks at the quantity and quality of training and research into future cybersecurity experts and measures. The cooperation pillar involves how much companies and agencies are cooperating both nationally and internationally. Combined, these metrics give a good comparison basis to determine how well countries are managing their cybersecurity.

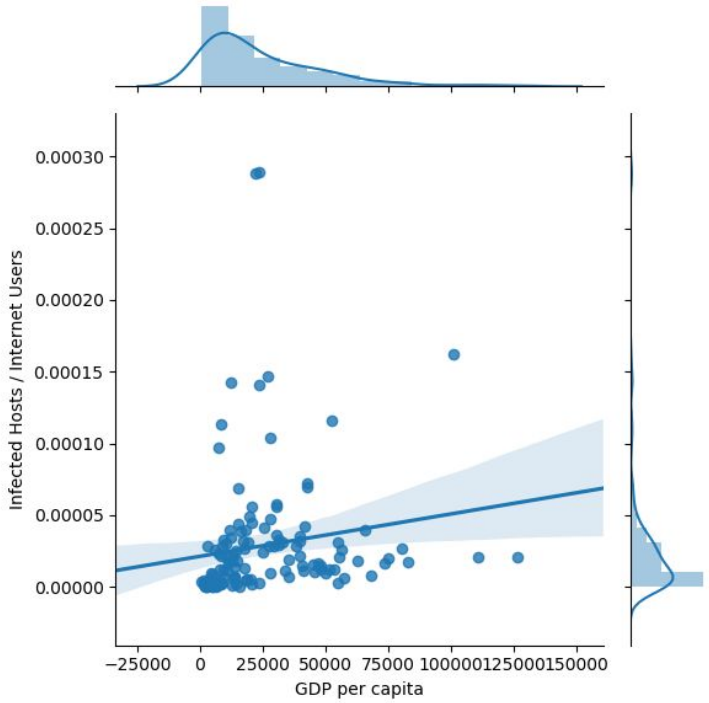
When correlated with the Mirai security metric, we see a small positive correlation of 0.249 with p=0.004. **<Todo draw conclusions from correlation>. <todo: possibly explain/name some of the extreme outliers>**



Correlation between Global Cybersecurity Index and amount of normalized newly infected devices per country. The blue line represents a linear regression estimate through the data points and the blue area around it a 95% confidence interval created using bootstrap samples.

Gross Domestic Product

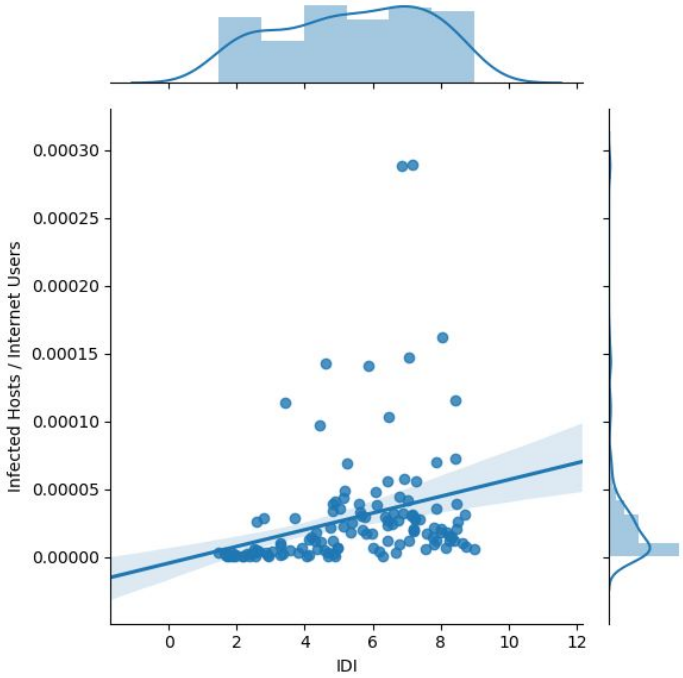
For the Gross Domestic Product we use the World Bank dataset of GDP normalized per capita[2]. When correlated with the Mirai security metric, we see a small positive correlation of 0.156 with p=0.0739. **<Todo draw conclusions from correlation>. <todo: possibly explain/name some of the extreme outliers>**



Correlation between Gross Domestic Product per capita and amount of normalized newly infected devices per country. The blue line represents a linear regression estimate through the data points and the blue area around it a 95% confidence interval created using bootstrap samples.

Overall ICT development

To measure overall ICT development of each country we use the ICT Development Index (IDI)[3]. When correlated with the Mirai security metric, we see a positive correlation of 0.292 with p=0.0007. **<Todo draw conclusions from correlation>. <todo: possibly explain/name some of the extreme outliers>**



Correlation between ICT Development Index and amount of normalized newly infected devices per country. The blue line represents a linear regression estimate through the data points and the blue area around it a 95% confidence interval created using bootstrap samples.

Conclusion

In this report we discussed several actors involved with our security issue: ISPs, device owners, and victims. For each actor, we discussed costs and benefits of possible countermeasures, and the externalities caused by them. We then performed a more in-depth analysis on the correlation between various datasets (GCI, GDP per capita, and ICT DI) against the infections in each country. We conclude that there is a positive correlation between the number of infections per user, and each of the datasets we analysedI.

References

[1] International Telecommunication Union. Global Cybersecurity Index 2018/2019. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx Annex B

[2] World Bank. GDP per capita, PPP. Retrieved from https://data.worldbank.org/indicator/NY.GDP.PCAP.PP.CD

[3] International Telecommunication Union. ICT Development Index 2017. Retrieved from https://www.itu.int/net4/ITU-D/idi/2017/index.html