Economics of Cyber Security
Assignment Block 4

Marco Dijkslag	Mathay Kahraman	Yoep Kortekaas	Sam Witt
s1743716	s1724665	s1719734	s1672509
4985028	5124182	4984595	5100356

October 14, 2019

1 Introduction

In this paper, the threat of DDoS attacks will be analysed for different actors. For each of the actors, a countermeasure is identified, with an analysis of the costs and benefits of that measure. Incentives for actors to take these countermeasures are explored, as well as any externalities that surround the DDoS attack security issue.

In our last research paper[3], we analysed the entity responsible for the DDoS attack problem and the strategies that this entity follows or can follow to deal with it. We identified manufacturers of IoT devices to be the problem owner, and suggested a number of risk strategies they could implement. The RoSI (return on security investment) was calculated for awareness campaigns, to increase the knowledge of the general public on how to secure their devices properly.

2 Actors

The three actors involved in the security issue that we can draw from our previous assignment are, the problem owner (i.e. the IoT device manufacturer), the government, IoT device owners. For each of the actors we will describe a countermeasure, what the distribution of costs & benefits is, the incentive to take the countermeasure, and reflect on the role of externalities around the security issue.

2.1 IoT Device Manufacturer

The first actor to discuss is the problem owner, as described in our previous paper[3], the IoT device manufacturer. In our previous papers the IoT device manufacturer was our problem owner, since they are responsible for manufacturing a secure IoT device and require that the users must change the default credentials of the IoT device.

2.1.1 Countermeasure

A lot of manufacturers set the default credentials to admin:admin or root:root for example. Botnets abuse these default credentials, an example of a botnet which abuses these default credentials is Mirai[2]. The countermeasure that the IoT device manufacturers could implement is the requirement that users must change the default credentials on the very first boot. Moreover, the user should not be able to use the device without changing the default credentials. Also during the installation of the device one can make the user aware that changing the default credentials is important and what could happen in case this procedure was not executed. This way we could also avoid that a lot of users set an easy password.

2.1.2 Distribution of Costs & Benefits

The costs of implementing the requirement of changing the default credentials on first boot are labour costs. This labour costs consists of implementing this solution and testing the implementation. There are no direct benefits for this solution, but there could be an indirect benefit for the manufacturer. Their manufactured devices will be less often part of botnets, and this could lead into less reputation damage for the manufacturer.

2.1.3 Incentive

Currently there is no large incentive for the IoT device manufacturer to implement this countermeasure, since there is no penalty when delivering the device without this countermeasure. When governments implement regulations for requiring the change of default credentials for example, IoT device manufacturers would have an incentive to implement this countermeasure, otherwise they would receive a penalty.

2.1.4 Externalities

An externality in this case is the victim of a DDoS attack performed by the botnet. An example of this would be Google or Facebook, since these are websites that have high traffic and thereby are often target of a DDoS attack. When these IoT botnets become smaller due to having that it is more difficult to infect an IoT device, these websites would have less DDoS attacks.

2.2 Government

The second actor we will discuss is the government. In our previous assignment we explained that the government can play an important role in reducing the security issue at hand [3]. We argued that it is in a government's interest to reduce the security issue, since critical infrastructures are attractive DDoS targets for attackers, and less DDoS attacks means that those critical infrastructures will likely experience less downtime.

2.2.1 Countermeasure

There are several different countermeasures that a government can take to mitigate the security issue, like creating a DDoS scrubbing centre to reduce DDoS attacks, or to run an awareness campaign to make their citizens more aware of the security of their (IoT) devices and have them change things like default passwords.

2.2.2 Distribution of costs & benefits

For the countermeasure we have chosen, the awareness campaign, costs would mainly be for the government themselves. It could be the case that the campaign is (partially) sponsored by DDoS victims, since they also benefit from a reduction in DDoS attack. But for now we assume that the costs for the awareness campaign will be paid by the government themselves. We identify that the benefits of such an awareness campaign will be for three different kinds of actors, namely the government, (large) DDoS victims, and IoT device manufacturers.

The first benefactor, the government, will experience a benefit from having the counter measure in place, since it means that less of the country's critical infrastructure will be down due to DDoS attacks.

The second benefactor, the (large) DDoS victims, also benefit from the countermeasure because they will have less downtime of their systems, and therefore have less loss of business continuity.

The third benefactor, the IoT device manufacturers, do not gain their benefit from less downtime due to less DDoS attacks. The benefit that they have is that safer IoT devices means that people are more incentivized for buying IoT devices, and therefore they can sell more devices and have more profit.

2.2.3 Incentives

We believe that there is an incentive for the government to take the countermeasure we described. One could argue that it is the responsibility of a DDoS victim to acquire DDoS protection, or to transfer the risk by purchasing DDoS insurance. We however think that it is part of the government's task to first of all make sure that critical infrastructure, such as banks or medical institutes are always available for their customers. Secondly, we also think that it is part of the government's responsibility to make sure that its citizens have free access to the internet. In a modern democracy it is important to have free access to all information, and DDoS attacks are an excellent approach to censor (unwanted) information on the internet.

2.2.4 Externalities

We can see two positive externalities for our measure. The first positive externality that we see is the benefit that we generate for the IoT device manufacturer. Due to the awareness campaign, IoT devices can be perceived as more secure by customers, and therefore IoT device sales might rise.

The second positive externality that we see is the benefit that we generate for DDoS victims. Due to the awareness campaign they might be hit less frequently by DDoS attacks, and if they are hit, they might be hit by less powerful attacks, which means it takes less effort to mitigate the attack. In both cases, it means they experience less downtime, which means that they lose less revenue.

2.3 IoT device owners

2.3.1 Countermeasure

The countermeasure that IoT device owners could take is to change the default credentials of their IoT devices. Also, if the device is able to, enable auto-updates, such that their devices are always running on the latest firmware/software.

2.3.2 Distribution of costs & benefits

It is difficult to measure the costs of such a countermeasure, since it depends on the user's skills whether they will change the credentials. We assume that the cost for changing the credentials is negligible. The benefit for IoT device owners from taking this countermeasure is that the device is no longer vulnerable to become part of a botnet because of the default credentials of the device. Therefore, their private network is also more secured.

2.3.3 Incentives

The incentive for taking this countermeasure, i.e. reducing the security issue, is that when an IoT device is vulnerable device for becoming part of a botnet due to not changing the default credentials, not only the device is vulnerable, but also the owner's private network. The private network is reachable from the internet via the IoT device, so devices that are normally not reachable from the internet are now visible. Thus if more device are vulnerable they could also get comprised. Besides devices getting comprised, it is also possible that users can no longer access their own devices because an attacker changed the settings. Furthermore, if the device becomes part of a botnet and therefore will help perform DDoS attack, also the device power usage and network bandwidth goes up.

2.3.4 Externalities

A negative externality of having this security issue is that the government and major platform owners are the target for more powerful DDoS attacks. A positive externality of taking the countermeasure is that these DDoS attacks will be less powerful.

3 Metrics

The type of actor we have chosen for this assignment is the government actor. The accompanying security metric can be found in Figure 1 and Figure 2. The metric shows us per country the amount of IP addresses that contacted the honeypot, normalized by the amount of IP addresses allocated to that country[1]. The countries are displayed with their 2 letter code[1].

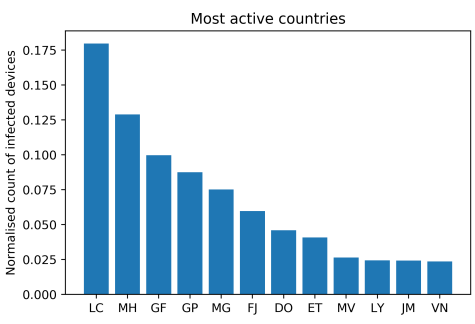

Figure 1: Normalised count of infected devices per country (bottom 12).

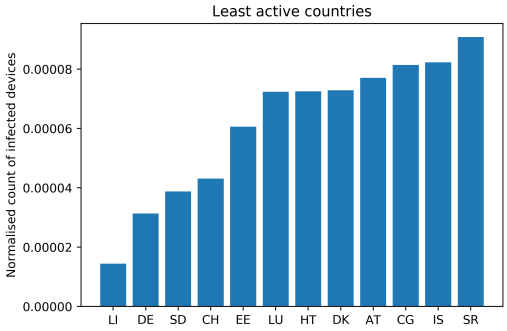

Figure 2: Normalised count of infected devices per country (top 12).

3.1 Factors causing variances

While we believe that our metric gives an accurate view of how well a country performs IoT security-wise, there are a few different factors that cause variance in the metric.

The first factor that has influence who we identified, is the amount of IP addresses that are allocated to a country. In a country that has a relatively large amount of IP addresses allocated in contrast to the amount of citizens, it is more likely that an IoT device gets its own public IP. In a country that has a relatively low amount of IP addresses allocated in contrast to the amount of citizens, it is more likely that one or more IoT device(s) are located behind a NAT[2].

Another factor is how populated countries are. In countries that have a higher population, the number of IoT devices will generally be higher than in countries with less residents. In general, more IP address space is assigned to countries with a relatively high population than to countries with a relatively low population.

The third factor that has influence we identified is the economical welfare in a country. In a country where the citizens are on average richer, there is also more budget for buying IoT devices. This results in that citizens buy better quality (name brand) devices, which (we hope) have better security.

3.2 Collected Data

In figure 1, we can see the countries with the most infected devices per x amount of devices in the country. The scale on the vertical axis means that in for example Saint Lucia (LC), per 100 devices, 18 of them have been infected with malware. Notice the difference in scale with figure 2, where for example Germany (DE), has only 3 infected devices per 100.000 devices. We can see here that in relatively small countries, with a relative small total number of possible devices, devices get infected with a much higher rate than in countries with a relative large number of total possible devices. An explanation could be that residents of smaller countries are generally not aware about any problems that rise from just connecting their IoT device without carrying out any forms of protective measures, like changing the default password. We do however have to take into account that the difference in total amount of possible devices is so big (Germany has roughly 6100 times more possible total devices than Saint Lucia), that the effects that might be causing the problem in Saint Lucia, could very well be present in Germany too. If we look at the

[1] https://www.worldatlas.com/aatlas/ctycodes.htm
[2] Network Address Translation

population in both countries, we see that Germany has roughly 460 times as many inhabitants as Saint Lucia, which also could prove that the problem is present in both countries.

3.3 Statistical Analysis

Not finished
We will calculate the Pearson's correlation between the economic welfare (GDP) and the ratio between the infected and normal IP addresses. We will also calculate the Pearson's correlation between the population of a country and the ratio between the infected and normal IP addresses. We have chosen for the Pearson's correlation, because it quantitatively describes the strength and direction of a relationship between two variables.

4 Conclusion

In our report we looked three different actors that are involved in our security issue. In subsection 2.1 we discuss the IoT device manufacturers. We discussed that the countermeasure that this actor can take is to have mandatory user/password change on first boot. We conclude however that there is currently no large incentive for IoT device manufacturers to undertake this action, due to a lack of consequences when the manufacturer does not implement the countermeasure.

In subsection 2.2 we discuss the government actor. For the government actor, the countermeasure that they can take is to organize an awareness campaign. We discuss that this has benefits for the government itself, but also for IoT device manufacturers and other DDoS victims. We conclude by stating that there is an incentive for the government to take this countermeasure, but we also think that the government will have to pay for the (majority of) the costs of the campaign.

In subsection 2.3 we discuss the IoT device owner actor. The possible countermeasure they can take is to change the default credentials of their IoT devices. We found that the costs is difficult to define, but on average it is negligible. The benefit for the IoT device owner of taking the countermeasure is that their device is more secure but also other devices in their private network.

In subsection 3.1 we discussed three different factors that is causing variance in the data. These factors are based on the amount of IP addresses allocated to a country, a countries population, and the economical welfare in a country. In subsection 3.2 we discussed the data that was collected for the given factors and what could explain the behaviours found. In subsection 3.3 we used the collected data to perform a statistical analysis using the Pearson's correlation coefficient.

References

[1] Ip address space per country. `https://ipfinder.io/countries/`. Accessed: 2019-09-30.

[2] J. Hendrickson. What is the mirai botnet, and how can i protect my devices? `https://www.howtogeek.com/408036/what-is-the-mirai-botnet-and-how-can-i-protect-my-devices/`, March 2019. Accessed: 2019-09-20.

[3] Y. Kortekaas, M. Dijkslag, M. Kahraman, and S. Witt. Economics of cyber security assignment block 3. `https://github.com/kahraman11/EOS2019/blob/master/Block%203/report/Economics_of_Cyber_Security_Final.pdf`, October 2019. Accessed: 2019-10-11.