Economics of Cyber Security

Assignment Block 3 (Draft)

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

September 30, 2019

1 Introduction

To combat the DDoS attack security issue, this paper will introduce an analysis of the entity responsible for the problem and the strategies that this entity follows or can follow to deal with it. In our last research paper [7], the DDoS security issue is explained, including an analysis of the actors and ideal security metrics that can be associated with DDoS attacks. The main actors were determined to be companies offering online services, people with IoT devices in their homes, manufacturers of IoT devices, criminals and governments. New metrics were also derived from an IoT honeypot dataset, to help identifying the problem and constructing methods to solve it.

2 Problem Owner

When defining the problem owner, it is quite essential to first explain what a problem owner is. The problem owner is responsible for an individual problem. The problem owner oversees the handling of the problem, bringing in analysts and specialists as needed to handle the problem. The Problem Owner is responsible for seeing that analysts and specialists bring the problem to a close[6].

As described in our previous paper[7], DDoS attacks are mostly due to having large botnets that gather new malicious devices by scanning the internet and attempting a lot of default credentials on potential vulnerable devices. These devices are vulnerable, since users do not change the default credentials and because manufacturers do not require to change the default credentials.

This brings us to the point where we have to describe who the problem owner is. One could discuss that the problem owner is the user of the device, since (s)he did not change the default credentials. On the other hand one could argue that the problem owner is the manufacturer of the vulnerable device, since he could require that users must change the default credentials on the first boot. We decided that the problem owner is the manufacturer of the device, since they are in first place responsible that the default credentials must be changed on first boot and they are responsible to repair vulnerabilities of their devices.

3 Differences in Performance

To visualize the differences in security performance with the data, the countries with the highest infected device ratio and the countries with the lowest ratio have been determined. The way this was calculated is by taking the number of IP addresses allocated per country [1], and then normalising the number of infected devices to the number of total possible devices in that country. The countries are displayed with their 2 letter code[1]. This shows which countries are doing well

[1]https://www.worldatlas.com/aatlas/ctycodes.htm

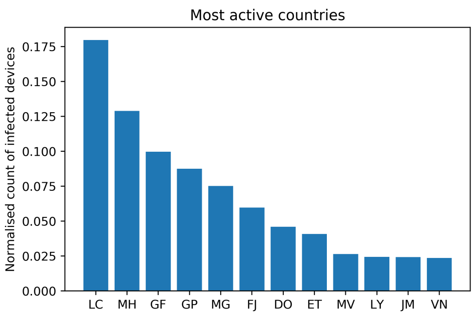

Figure 1: Normalised count of infected devices per country (top 12).

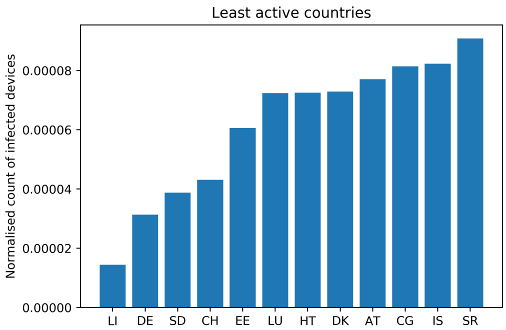

Figure 2: Normalised count of infected devices per country (bottom 12).

with respect to securing their devices, and which countries still have a lot to improve. 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 1, 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 devices, devices get infected with a much higher rate than in countries with a relative large number of total devices. This would mean that the population in such small countries is relatively uneducated on device security measures, or network security measures in general. An explanation could be that people 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. In the following sections, strategies to deal with this problem will be explained. 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 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.

4 Risk Strategies for Problem Owner

To reduce the security issue that was measured and described in the previous section the problem owner can implement several risk strategies. Here we describe four of these risk strategies that can be implemented by the problem owner.

The first strategy that can be implemented is for a user on installing an IoT device, i.e. from such a manufacturer described in section 2, to make changing the default username and password of the device obligatory. Moreover, the user should not be able to use the device without changing it. Also during the installation of the device one can make the user aware that changing it is important and what could happen in case this procedure was not executed. This way we can also avoid that a lot of users set an easy password.

As a second strategy that can be implemented is to close the telnet (port 23) on the device. This port is often abused by botnets to infect other devices over this channel. For the average costumer there is no need to leave this port open, whereas most customers would not know there exists such a port, what a port is in general or what it can be used for.

Since most IoT devices use the same port to access the application running on the device via the internet, the port on which the application is reachable could be randomized. Implementing this strategy makes it harder for an attacker to get access to a (probably insecure) IoT device, since scanning the whole port range of a device can take a significant amount of time.

Lastly, the manufacturer of IoT devices can implement a strategy to provide long-term-support (LTS) for their devices. They can bring out patches and let users update their devices when they know there is a malfunction or when a security flaw has been discovered. Also by providing updates to their customers it can be used as a method to set a device back to its factory settings (or any other preferable state) when it is discovered it got infected by a botnet. Furthermore, an option to auto run updates for these devices makes it easier for the user to maintain their devices and the manufacturer does not have to encourage users to update their devices, since users can be reluctant to update their device.

5 Other Actors

Next to the problem owner, the manufacturer of the IoT device, there are other actors that can influence the security issue we measured in our previous assignment. In this section we will define these other actors, and why this issue is relevant to them.

Government

The first actor we will discuss is the government. There are several reasons why this issue is also relevant to governmental institutes. The first and most important reason is that mostly critical parts of a nations infrastructure, such as governmental institutes[8], but also banks [4] are popular DDoS attack targets. Since these targets are a critical part of the national infrastructure, it is in the government's best interest to protect these assets from DDoS attacks.

Another reason for governments to partake in reducing unsafe IoT devices (and there reducing DDoS attack strength) is to prevent certain criminal activity. Next to using DDoS to disrupt critical services, it can also used by criminals to cover up other shady activities like data theft [9]. Reducing (the strength of) DDoS attacks can lead to less attacks, or at least less obfuscation of the actual attacks, which in the end will lead to an reduction in organised IT crime.

Major online platforms

The second actors we will discuss are major online platforms. Under major online platforms we consider social media platforms such as Facebook and Twitter, but also online retailers like Amazon, hosting providers like OVH, DNS providers like Dyn and any other large company that gets the majority of their business from online services. The main reason why these platforms should be interested in reducing the security issue is that DDoS attacks threaten their main source of income. These platforms can only earn revenue when their services are available, and DDoS attacks undermine the availability of their services. Repeated unavailability of online services can even lead to permanent loss when customers switch to a different platform with better up-time.

For hosting and DNS providers this risk of permanent losses is even larger, since the unavailability of their services can lead to unavailability of other online services. An example of this happening is when DNS provider Dyn got hit by a 1.2 Tbps DDoS attack in 2016, leading to unavailability major online platforms like Twitter and Netflix [11].

IoT device owners

The last actor we are discussing are the owners of the IoT devices. Reducing the security issue is relevant to them too for a couple of reasons. The first reason is that having a vulnerable device in their private (home) network, gives an attacker entry to the private network. This means that devices that are normally not visible to the internet, now can be reached, and possibly compromised, by an attacker. So reducing the security issue means that IoT device owners have less risk of other (personal) devices getting hacked.

A second reason why reducing the security issue is relevant for IoT device owners has to do with the functioning of the IoT device. When such an IoT device is compromised, an attacker (usually) has full control over the compromised IoT device, meaning they can execute whatever action they like. This can lead to an increase in power usage, meaning that the usage of the IoT device is more inconvenient. A more serious issue is that an attacker can make the IoT device unresponsive, or even change the functionality of the device, e.g. giving back incorrect temperature readings for a temperature sensor.

Now that we have an idea of what kind of other actors this security issue is relevant for, we will in the next section we will discuss what kind of strategies these "other actors" can exercise to reduce the security issue at hand.

6 Risk Strategies for Other Actors

The previous section describes which other actors there are. This section will describe what kind of risk strategies these other actors can adopt to tackle the problem of DDoS attacks.

6.1 Actors with different strategies

The first other actor that has been defined are governments. Governments are often target of a DDoS attacks[3] and to prevent these attacks they could start an awareness campaign under their citizens such that the owners of potential malicious devices are aware of the risks of not changing the default credentials and updating their devices such that they are always running at the latest released software version.

The second other actor are the IoT device owners. As described in the previous paragraph, these IoT device owners should change the default credentials of their IoT devices and enabling auto-updates on their devices such that their devices are always running on the latest released software version.

The third strategy is based on two different actors: governments and major platform owners like Google and Facebook. These two actors could put pressure on manufactures of vulnerable IoT devices such that they invest more resources in the security of their IoT devices.

6.2 Changes in strategies

Although there exists some campaigns by governments to raise awareness for people's online security, we are not aware of a campaign that is targeted at people's IoT devices. Meaning there is no risk strategy in place from the government perspective to tackle the problem of IoT devices getting infected by botnets.

Most users do not change the default credentials of their IoT devices and are not aware of the risks involved in not doing this. Meaning there is no risk strategy in place of the customers of these IoT devices regarding the security of the device, and no intention to do so either. If the users were aware of the security issues of their IoT devices they are more likely to keep them up-to-date and change the default credentials.

Major platform owners could implement the strategy of putting pressure on manufacturers of IoT devices to keep the devices security up-to-date, since otherwise they might have not intention for this. We are not aware of existing major platform owners that actively put pressure on manufacturers to keep their devices secure.

7 Return on Security Investment

The risk strategy that will be discussed in this section is the risk strategy of major platform owners. These major platform owners are a high class target for DDoS targets and that means that they are often targets of high scale DDoS attacks. Their return on investment is likely to be high if they can prevent losses due to DDoS attacks. For our ROSI calculation we will focus on costs and benefits in the Netherlands, since we could find the most literature regarding costs and benefits for DDoS attacks and campaigns in the Netherlands.

7.1 Costs

To decrease the amount of DDoS attacks the major platform owners could start an awareness campaign. An awareness campaign obviously costs money. To determine the amount of costs to start and maintain a campaign we have taken a look at the cost that SIRE[2] has when creating a campaign in the Netherlands. In 2011 they have created four large campaigns. The total costs

[2]SIRE is a Dutch organisation that creates media campaigns regarding important societal issues[10]

of these four campaigns were 9.5 million euros[2], meaning that the average costs of these four campaigns is roughly 2.4 million euros.

To calculate the average DDoS attack cost for businesses is quite difficult. Fortunately, NBIP has done a research in this area in the Netherlands and came to the conclusion that in total there was as damage of 425 million euros and the amount of damage per attack is approximately 1.8 million euros[5]. From this we can conclude that in 2018 there was an average attack frequency of 237 attacks.

7.2 Benefits

There are two approaches to calculate the benefits of this awareness campaign: the approach where there are less DDoS attacks due to having less infected devices in a botnet and the other approach is that the DDoS attacks that are still there are less powerful than before and thereby easier to reflect.

To calculate the benefits when there are less DDoS attacks performed, is quite easy to calculate: for each DDoS attack less then in the same period before is a saving of averagely 1.8 million euros. To define how much less number of DDoS attacks there are after the awareness campaign compared to before is difficult to calculate. A way to determine this is just by guessing a (pessimistic) amount of around ten percent.

To calculate the decrease in strength of DDoS attacks we have to make a guessing like described in the previous paragraph. To set this decrease value to a (pessimistic) amount we could set it to around 15 per cent.

7.3 Result

In order to calculate the RoSI value, we use the following formula:

$$RoSI = \frac{ALE_0 - ALE_s - c}{c}$$

To calculate the RoSI, we need to calculate the ALE_0 and the ALE_s. ALE stands for Annualised Expected Losses and is calculated by multiplying the Impact (Unit) by the Probability (Annual).

First we calculate the ALE_0, this stands for the ALE without the security measures in place. The impact is will be set to the average costs of a DDoS attack, which is 1.8 million euros. The probability will be set to the amount of attacks (237) divided by the amount of targeted .nl domain names (770.000) which is 0.03 per cent. This results in an ALE_0 of (0,0003*1.800.000) 554.

Next it is time to calculate the ALE_s, this is the ALE with the security measures in place. As described in the previous section the amount of DDoS attacks will decrease probably with ten per cent which results in a total amount of (237*0,9) 213 DDoS attacks and which will result in an average cost of (1.800.000*0,85) 1.530.000 euros per DDoS attack. The probability of being attacked by a DDoS attack is set with these values to (213/770.000) 0.028 per cent. This results in an ALE_s of (0,0028*1.530.00) 423.

The last step is to calculate the RoSI, which stands for Return on Security Investment and is calculated by: $\frac{ALE_0 - ALE_s - c}{c}$. The c stands for costs and is defined in the *costs* section above by 2.4 million euros. This results in a RoSI of: $\frac{554-423-2.400.000}{2.400.000} = -0.99$.

The result of the RoSI is negative, which means that it is not worth for a single company single-handely to invest in a security awareness campaign. This can be easily explained, because the costs of a awareness campaign is rather large compared to the in risk of a DDoS attack and the amount that a DDoS attack costs. To let the RoSI result in a positive result it would be smarter for companies to invest together in one awareness campaign such that the costs for the companies decreases.

When creating the awareness campaign with all the targeted devices (770.000) the c in the formula of RoSI will decrease to (2.400.000/770.000) 3,12 euros. Which results in a RoSI of 40,99.

8 Conclusion

In this report we have defined and discussed several security investment & management related concepts regarding our security issue. In section 2 we presented the IoT device manufacturer as problem owner, since we think that it is the manufacturer's responsibility to release security patches for their devices, and make sure IoT device owners change default credentials on first boot.

In section 4 we discuss which risk strategies the problem owner (the IoT device manufacturer) can take to reduce the security issue. We discuss three different risk strategies, namely changing default credentials on boot, closing Telnet/remote access ports and lastly providing long term (security) support for IoT devices.

In section 5 and section 6 we discussed which other actors, next to the problem owner, (should) have interest in, and can partake in reducing the security issue. We identified the government, major online platforms and IoT device owners as potential other actors. Risk strategies that they can exercise are (among others) doing awareness campaigns, and putting pressure on IoT device manufacturers to secure IoT devices better.

Finally in section 7 we took on of our risk strategies, and we computed the *Return On Security Investment (RoSI)* score for that strategy. We choose to compute the RoSI for the awareness campaign strategy, looking specifically at the Netherlands since most of our sources regard the Netherlands. The result of our RoSI calculation is that the awareness campaign gets a score of -0.99 for when a single company funds the entire awareness campaign. When the cost of the campaign is distributed over all in 2018 targetted companies, the RoSI score of the risk strategy is +40.99.

References

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

[2] Jaarverslag 2011. `https://sire.nl/wp-content/uploads/2017/10/2011-2.pdf`, Aug 2012. Accessed: 2019-09-30.

[3] Cyber attack shuts down many government websites in finland. `https://yle.fi/uutiset/osasto/news/cyber_attack_shuts_down_many_government_websites_in_finland/10350316`, Augustus 2018. Accessed: 2019-09-27.

[4] Nieuwe ddos-aanval op abn amro, ing, rabo en belastingdienst. `https://nos.nl/artikel/2214537-nieuwe-ddos-aanval-op-abn-amro-ing-rabo-en-belastingdienst.html`, Jan 2018. Accessed: 2019-09-29.

[5] N. Boerman, M. Henneke, G. Moura, G. Schaapman, and O. de Weerdt. The impact of ddos attacks on dutch enterprises. `https://www.nbip.nl/wp-content/uploads/2018/11/NBIP-SIDN-DDoS-impact-report.pdf`, Nov 2018. Accessesd: 2019-09-30.

[6] IBM. Role: Problem owner. `https://www.visioline.ee/itup/itup/roles/problem_owner_3556C72.html`. Accessed: 2019-09-26.

[7] Y. Kortekaas, M. Dijkslag, M. Kahraman, and S. Witt. Economics of cyber security assignment block 2. `https://github.com/kahraman11/EOS2019/blob/master/Block%202/report/Economics_of_Cyber_Security_Final.pdf`, September 2019. Accessed: 2019-09-26.

[8] D. McGuinness. How a cyber attack transformed estonia. `https://www.bbc.com/news/39655415`, Apr 2017. Accessed: 2019-09-29.

[9] P. Roberts. Ddos as a cover for data theft. `https://digitalguardian.com/blog/ddos-cover-data-theft`, Sep 2015. Accessed: 2019-09-29.

[10] SIRE. Veelgestelde vragen. https://sire.nl/veelgestelde-vragen. Accessed: 2019-09-30.

[11] N. Woolf. Ddos attack that disrupted internet was largest of its kind in history, experts say. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet, Oct 2016. Accessed: 2019-09-29.