WM0824TU Group 9
Block 4

Chris Berg, 4216776
Martin Koster, 4371011
Radinka Yorgova, 4952545
Wilko Meijer, 4224426

October 22, 2018

1 Introduction

In the last report we saw how the risk strategies shaped the variance of the security performance with regard to a metric. We will now explore the factors which could cause these variances. We will start by describing the main actors involved in the security issue and the effects they have on each other. We focus on some of their countermeasures and the distribution of the resulting costs and benefits. The first part is concluded with a short discussion considering the externalities affected by solving the security issue.

In the second part we consider one of the actors. We identify different factors that could cause the variance of the chosen metric and explore the effect of these factors using statistical analysis.

2 Actors

The actors we discuss in this report are: ISPs, device manufacturers and the government. These three actors are able to influence the spreading of the Mirai malware by infecting new devices and increasing the size of the corresponding botnets in a direct or indirect way.

2.1 ISP

The first actor we are going to discuss is the problem owner, the ISPs. A countermeasure they could take to mitigate the security issue is by implementing a security investment which detects bots and therefore can block the botnets. In [1] some metrics to do this are discussed. Every bot of the botnet uses the services of an ISP, so the ISP is the ideal place to detect the bots and therefore able to stop botnets. Because the ISP is the actor that can have the highest influence in solving the problem, the ISP will be considered the problem owner.

Therefore, we will continue in the next section by describing the effect of security efforts of the ISP on the spread of Mirai-like botnets.

In [3] we see a good overview of the general costs and benefits for IT and Non-IT companies which comes with such a security investment (Figure 1).

Figure 1: Comparison of IT and Non-IT costs and benefits

Security Strategy	IT Impacts	Non-IT Impacts
Proactive	• Cost: Cutting-edge hardware and software (likely more expensive than well-established solutions) • Cost: Information gathering, installation, debugging, and maintenance costs (labor)	• Cost: User inconvenience
	• Benefit: Decreased need for reactive labor	• Benefit: Regulatory and reputation benefits • Benefit: Fewer business interruptions
Reactive	• Cost: Infrastructure (mostly labor) resources needed to respond quickly and effectively • Cost: Resources (labor) needed to repair damaged systems and data	• Cost: More events, and thus a likely increase in down time • Cost: Potential damage to reputation
	• Benefit: Decreased investments in proactive (risky) solutions	• Benefit: User convenience • Benefit: Flexibility to accommodate diverse business environments

The ISPs themselves are not the victim of such botnet attacks and as we see in Figure 1 there is mainly costs connected to such a security investment. Therefore the ISPs do not have an incentive to implement a security investment to prevent mitigation. The main benefit for the ISP is prevention of a potential reputation damage. Later on, we will discuss how the ISP as innocent third party can be enforced to tackle this security issue. When an ISP decides to implement this security investment, this could result in the following costs:

- costs for acquisition of the detection and blocking hard- and software
- costs for acquisition of Network Intrusion Detection Systems (IDS)
- costs for installation and maintenance of the security system
- the training of the employees and the change of protocols

We have already mentioned that there is little benefit for the ISP to counter the security investments of preventing the spread of botnets apart from some reduced chance of reputation damage.

The countermeasure of the ISPs do however have a positive externalities. There

are some third parties who benefit from the ISP implementing this security investment. Such third parties are companies which are potential victims of the botnet attack. For the end-users of infected devices there can be costs attached with the security investment and so a negative externality. When their device is detected being recruited in a Mirai-like botnet, the end user has to reset it, which is an indirect (small) cost, or the end user has to purchase a new device which is a larger cost.

2.2 Device Manufacturer

Next are the device manufacturers. Bad security, like using default passwords, is the main reason IoT devices are infected. This is something where device manufacturers can contribute to mitigate the risk of the botnet spreading and therefore mitigating the risk of a botnet attack. With a better security, attackers have to do much more to infect such a device.

As we saw with the ISPs, device manufacturers do not have incentives to implement this security measurement, since they do not suffer from the botnet. Their only loss would be reputation damage. However, regulation can create new incentives for the manufacturers.

The main reason why device manufacturers do not want to implement the security issue is because it will give costs with relatively little benefit. They have to invest in the security, it has to be implemented in every device and the employees of the manufacturer have to be trained. The only benefit they have is the prevented reputation damage. The ISPs and the government will not have any costs from this. The ISPs will have a little benefit. Since the botnet spreading is more difficult for attackers with more secure devices, the botnet attacks will also be more difficult. Therefore botnet attacks occur less, which means a decrease of reputation loss for the ISPs. The government will also benefit since again they can also be a victim of botnet attacks.

The implementation of the security investment will have the same positive externality as we saw with the countermeasure of the ISPs. Also now the end users can experience a negative externality. For example, the default passwords are not secure so every end user is now obliged to create a login, which takes an indirect (small) cost. Also it is possible that making such an improved device requires more/different material which is bad in terms of the environment.

2.3 Government

The last actor we discuss is the government. The government will not have a direct way on influencing the security issue, but a more indirect way. We saw in the previous sections that ISPs and device manufacturers won't have any incentives to implement the security investments. The government have the authority to introduce additional regulations and to initiate changes in the law which force ISPs and device manufactures to limit the spread of botnets. Then ISPs and device manufactures are enforced to apply security investments. This is also called indirect intermediary liability.

The question now is: does the government has any incentive to make this happen? The government itself can be a victim of botnet attacks. Besides that, the government can feel responsible of the attacks which happen in their country. However, making such a regulation is not easy, since it is not easy to specify exactly to what an ISP or device manufacturer has to comply to.

Assume such a regulation is made, the government won't have any costs from it. The benefits is the same as discussed in the previous sections, which says that the government does now have a less chance to be a victim of a botnet attack. The costs are all for the ISPs and the device manufacturers which have to implement the security investments. However, they will also have some benefits in terms of the prevented reputation loss.

Since this tactic of mitigating is using the security investments of the other actors, the externalities will be the same as for those investments (discussed in the previous sections).

3 Security Performance

3.1 Identify different factors explaining (causing) the variance in the metric

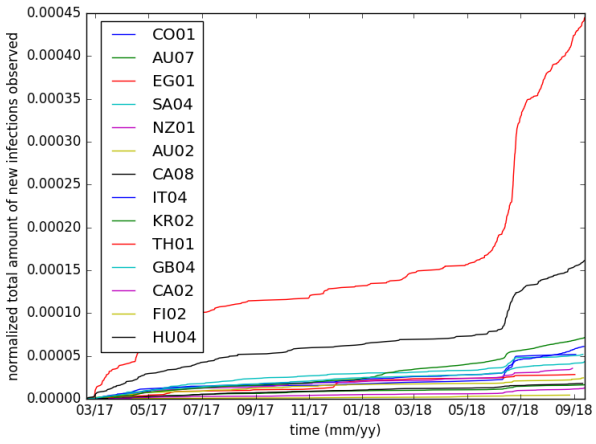

Figure 2: Metric applied on a random selection of ISPs

The metric we choose for the analysis in this report is a modification of the metric from the last report. More precise, the considered metric is of total amount of IPv4 addresses, showing behaviour related to Mirai malware infection, newly observed per ISP over time and normalized on the size of the ISP, measured as the total amount of IPv4 addresses issued by that ISP.

Considering the influence of the security performance of different actors on this metric there can only be one actor whose security performance influences the metric the most: the ISPs. The manufacturers do not influence the autonomous system being used that much, except for the geographical location of their market overlapping with the location of the market of an ISP. Governments have an influence on the ISPs through regulations, but they can only influence the security performance of the ISPs by regulation. The security performance of the government has little to do with the metric. Furthermore, security breaches at ISPs such the router vulnerability at the Telmex in April 2018 [2] are clearly visible in this metric.

Different factors that could cause variance in the metric could be:

- Difference in countries (should the ISPs be located in different countries)
  - Privacy laws
  - Institutional power (ability to enforce laws)
  - Income per capita
- The size of client base of ISPs
- Security breaches in the ISPs
- Security investments of the ISPs

The Privacy laws and Institutional power is well studied and captured in the Global Cybersecurity Index by the International Telecommunication Union. The report [6] presents the methodology which is used for calculating this index. Here we cite the brief description of the five pillars used there:

"1. Legal: Measured based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime.

2. Technical: Measured based on the existence of technical institutions and frameworks dealing with cybersecurity.

3. Organizational: Measured based on the existence of policy coordination institutions and strategies for cybersecurity development at the national level.

4. Capacity Building: Measured based on the existence of research and development, education and training programmes; certified professionals and public sector agencies fostering capacity building.

5. Cooperation: Measured based on the existence of partnerships, cooperative frameworks and information sharing networks."

3.2 Statistical Analysis

3.2.1 Size of ISPs

The size of the ISPs is measured in the amount of IPv4 addresses they are hosting. Data on their size was collected using *pyasn* [4] by summing the sizes of the autonomous systems owned by the ISPs. It quite hard to do a statistical analysis over time for the sizes of ISPs. Therefore we calculate the correlation

of the total amount of new infections observed in the data set, and the size of the ISP at the time of the last entry of the data set. The resulting scatterplot can be found in Figure 3. It is slightly zoomed, 4 data points are out of view. There doesn't seem to be a high correlation between the size of the ISP and the total amount of new infections observed as can be seen by the spread of the data points and the (red) linear regression line. This is confirmed by calculation the Pearson correlation for this factor, which is 0.1027 with a p-value of 0.1058. This correlation doesn't get much better by only looking at the cluster of data, for infections a maximum of 1 000 infections and 200 000 000 ISP size, the correlation is 0.3562 with a p-value of 0.0000. Therefore it can be concluded that the size of the ISP doesn't have a significant impact on the variance of the metric.

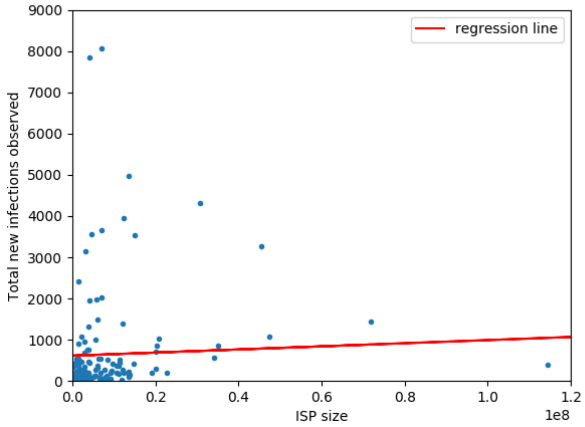

Figure 3: Scatterplot of ISP size (IPv4 addresses) and total amount of new infections observed for the same ISP (zoomed)

3.2.2 Income per Capita

In the previous section we discussed a factor which is dependent on the ISPs. In this section the factor will be dependent on the country of the infected devices. The factor we take into account in this section is the income per capita. The data we have used is the GNI (Gross National Income) per country and is collected from the World Bank [5]. First, the normalized amount of infections observed per ISP (infection rate) was calculated. After that a comparison could be made between those results and the GNI of the matching country. This is done via a scatter plot which is shown in figure Figure 4. As for the previous factor, also this factor seems to have little to no correlation with the number of infections. To be sure we made some calculations to support this claim. The Pearson correlation for this factor is -0.0558 and the p-value is 0.3814.

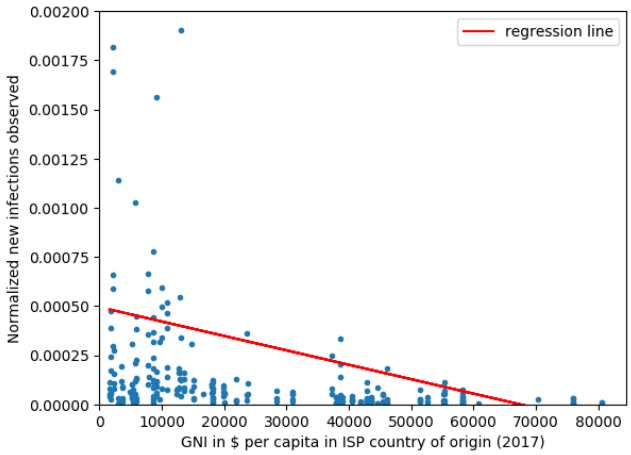

Figure 4: Scatterplot of the GNI of the ISPs origin country and infection rate of the same ISP

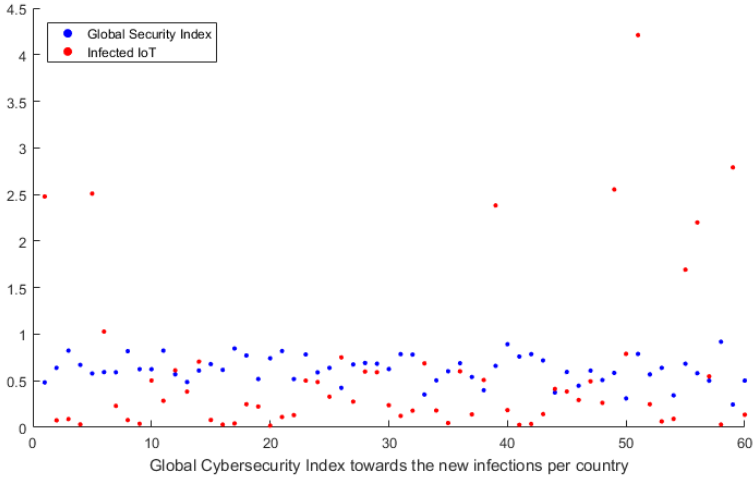

Figure 5: Scatterplot of the newly Infected IoT and the Global Cybersecurity index per country

3.2.3 Global Cybersecurity Index

The Privacy laws and Institutional power as factors that could cause variance in the metric are included in the Global Cybersecurity Index. Therefore we use the index per country given in the report [6] to explore a dependency between

the results in our metric with the general Cybersecurity level in the country. For this purpose we consider the total number of the newly observed infected devices per ISP summarized per country and normalized over the ISP sizes. First in Figure 5 we give an overview of this number towards the Global Cybersecurity Index. There is clearly a correlation between the level of the Index and the number of the infected devices. In the majority of the countries the high index corresponds to a low level of the new infections. There is one exception on country 51 where the high level of the index is in a contradiction with the high level of Mirai botnet spread. That could be caused by a change of the strategy of another actor involved in the security issue or simply by manipulated data given to the authorities. In the Figure 6 we give the correspondence of the Global Cybersecurity Index towards the normalized total number of the newly infected IoT with the Mirai malware per country. The regression line is also obtained and displayed. In comparison to the other factors this seems in higher correlation with the number of infections. The Pearson correlation for this factor is -0.1923, with a p-value of 0.1408 which still is pretty low for a conclusion for high correlation. We have to point that our analysis dials with data from a different time. The data for our metric is from the second half of 2018 whereas the Global Cybersecurity Index is for 2017 but issued in 2017 which means that the data used for the report are even older.

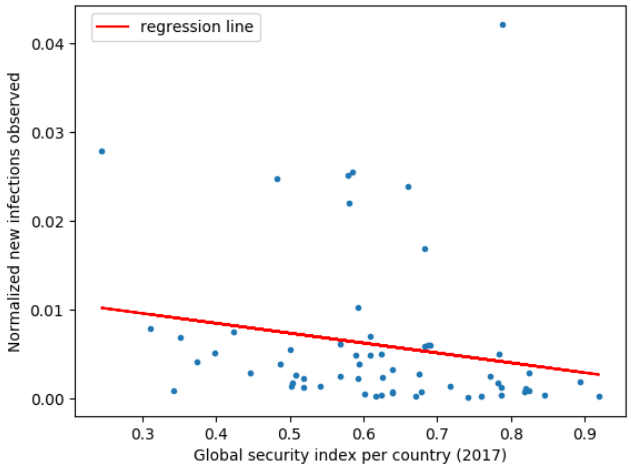

Figure 6: Scatterplot of the newly Infected IoT in connection to the Global Cybersecurity index per country

4 Conclusion

In the security issue of the spread of Mirai-like botnets, there is no actor with a financial incentive of making security investments to prevent the spread of these botnets. The externalities of this ignorance are for example business suffering

under a range of botnet-attacks. Therefore, one of the actors should be made responsible to solve the problem as an innocent third party. This actor should be the ISP, because of its ability to influence the spread of these botnets. The conjecture of ISPs being the problem owner is based on huge increases in botnet spreading being linked to security flaws in ISPs. Statistical analysis of different factors against the spread of infections reveals that it is hard to provide solid statistical proof that security investments of ISPs are related to the decrease of the spread of Mirai-like botnets through that ISP. This is the result of most factors being influenced by many other influences, compared with which the IoT devices only have a very small effect. Therefore, some experiment might be set up to reduce the botnet traffic within the autonomous system of that ISP. This should take place in order to create an example from which, depending on the effectiveness of the experiment, legislation may or may not be enforced onto ISPs.

References

[1] Akiyama, M., Kawamoto, T., Shimamura, M., Yokoyama, T., Kadobayashi, Y., Yamaguchi, S. (2007, January). A proposal of metrics for botnet detection based on its cooperative behavior. In Applications and the Internet Workshops, 2007. SAINT Workshops 2007. International Symposium on (pp. 82-82). IEEE.

[2] Zack Whittaker, "Over a million vulnerable fiber routers can be easily hacked", https://www.zdnet.com/article/over-a-million-vulnerable-fiber-routers-can-be-easily-hacked/, accessed 5 Oct 2018.

[3] Gallaher, M. P., Rowe, B. R., Rogozhin, A. V., & Link, A. N. (2006). Economic Analysis of Cyber Security. RESEARCH TRIANGLE INST (RTI) RESEARCH TRIANGLE PARK NC.

[4] Economics of Cybersecurity at Delft University of Technology. "pyasn 1.6.0b1 - Offline IP address to Autonomous System Number lookup module." https://pypi.org/project/pyasn/.

[5] The World Bank. GNI per capita, Atlas method (current US$).

[6] International Telecommunication Union (ITU). "Global Cybersecurity Index (GCI) 2017", www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf