WM0824TU Group 9
Block 4

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

October 15, 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. Here will explore the factors why these variances occur. For this we first describe in details three of the main actors involved in the considered 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. Moreover for each of the three actors the role of the externalities around the security issue is discussed shortly. In the second part we consider one of the actors. There we identify the different factors causing 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: ISP's (the problem owner), device manufacturers and the government. After going into details for each of them we focus on ISP's. For sake of completeness we recall the security issue: spreading of the mirai malware by infecting new devices and increasing the size of the corresponding botnet(s).

2.1 ISP

The first actor we are going to discuss is the problem owner, the ISP's. 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] they discuss some metrics to do this. 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.

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 ISP's are not the victim of such botnet attacks and as we see in Figure1 there is mainly costs connected to such a security investment. Therefore the ISP's have not many incentives to implement a security investment mitigating the security issue. The main benefit for them which is not mentioned in the table is prevention of a potential reputation damage. We will see later how they can be enforced.
When an ISP decides to implement this security investment, it will give the ISP many costs as:

- costs for acquisition of the detection and blocking hard- and soft- ware;
- 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 the only benefit is with regard to the prevented damage loss.

For the device manufacturer this will not give any costs and benefits. The government will have some benefit, because there are a potential victim of botnet attacks. There are no costs for the government.
The ISP's do have a positive externality. 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, 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. Mainly the infected IoT devices have bad security, with for example default passwords. 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 effort to infect such a device.
As we saw with the ISP's, device manufacturers will not have incentives to implement this security measurement, since it does not suffer from the botnet. Its only loss would also be reputation damage. Also this can be enforced, which will be discussed in the next section.
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 ISP's and the government will not have any costs from this. The ISP's 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 attack occur less, which means a decrease of reputation loss for the ISP's. The government will also benefit since again they can also be a victim of botnet attacks.
The implemention of the security investment will have the same positive externality as we saw with the ISP's. 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/diiferent 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 ISP's 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 low which force ISP's and device manufactures to limit the spread of botnet. Then ISP's 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 ISP's 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

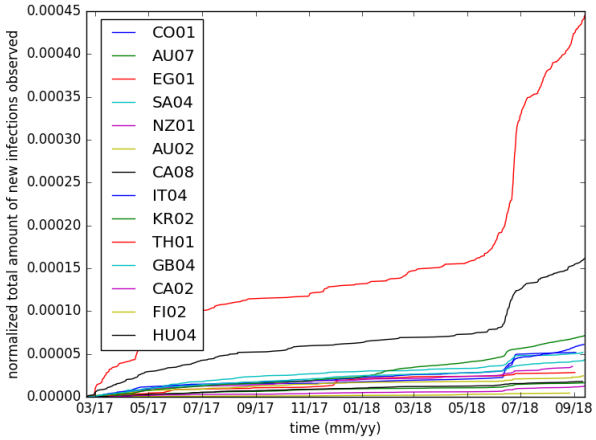

Figure 2: Metric applied on a random selection of ISP's

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

3.2 Collect data for one or several of these factors

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.