Economics of Cyber Security

Peer Review Group 1 (Mirai)

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

September 25, 2019

1 Summary of the assignment

To summarize this paper, we start of with the motivation. The motivation of this research is that Mirai malware is installed on a lot of vulnerable IoT-devices and that the huge spread of this malware is concerning. ISPs could be a possible connection to stop preventing the spread of Mirai malware. The methods which the authors have used are a graph that shows the amount of infected devices per country and a stacked bar chart that shows the port distribution over time. The conclusion of the research is that ISPs should design effective countermeasures against Mirai such that major internet services can be run safely. As the graphs in the paper shows, ISPs in Armenia and Vietnam should perform more work to stop the spread of Mirai. Finally, the authors of the papers would like to motivate the ISPs with their metrics to actively try to stop the spread of Mirai.

2 Strengths of the assignment

The clearest strength of the assignment is how the theory is connected to the real world of ISPs. The paper discusses how the metrics they found can be directly used in various ways by ISPs. This shows a definite connection with the real world, makes the paper less of an abstraction and clearly indicates the usefulness of the work.

When reading this paper, you immediately notice that they have clearly described what the motivation, research and conclusion is of their paper. Almost everything (except the following major and minor issues) was described clearly and extensively and thereby we could not establish a lot of major and minor issues. Given below is an enumeration of the strengths of this paper:

1. Clear connection between theory and practicality
2. Clearly described the motivation, research and conclusion
3. Used a lot of sources to strengthen their claims
4. Clearly described in section *Metrics in Practice* how they were going to count the amount of botnets and what the (dis)advantages are of this way.
5. Clearly explained why and how there is a peak in figure 1 on page 7. (release of source code of Mirai)
6. Good explanation of why the port distribution of Mirai has been changed over time in figure 2 on page 8. (new versions of Mirai)
7. The conclusion clearly follows the results that has been described in section *Data Analysis* and thereby looks trustworthy.

3 Major issues

1. At the end of the *Introduction and scope* section, the authors of the paper suddenly answer the questions: *Whose security? Security of which values? Security from what?*, without explaining where these questions come from or how they are relevant. It is good that these are mentioned, but the way in which this is done is very confusing as there is no explanation given. Also no analysis of other potential issues and actors has been done. No references are made to a potential source that explains these.

2. In section *Developed metrics* there are two tables which use the SMART characteristics. They are used without a source or explanation, and even without using the keywords that the letters in the abbreviation stand for. For people not knowing about this framework, this is confusing and here too, no reference is made to a source that further explains it.

4 Minor issues

1. Figure 1 on page 7 has used colours that are quite hard to distinguish. Using bright different colours would have greatly helped to distinguish the different countries better.

5 Typos

On page 3, line 32 change *they're* to *they are*.