

Peer review of Group 5  
Economics of Cyber Security -Assignment block 2  
28/09/2015

## **1) Summary**

In this report, the main security problem is the phishing. The stakeholders given by the group 5 are Internet providers, Email providers, banks and users of these services. They start by defining the word “phishing” and explain why they decided to choose this security issue. They focused on popular targeted countries, for example to list criminal groups locations. Then, they present the ideal metrics from the model “cost of security, security level, benefit of security”.

Thus, they proposed a great number of metrics, and they finally chose to characterize these metrics :

- Uptime of phishing website per targeted countries
- Number of Internet users per targeted/origin country
- GDP per targeted/origin country and presence of normalised targeted country
- Number of attacks per country/region, normalized by the number of local internet users

Next, they describe the data statistics given by the websites PhishTank, CleanMX, and doshi.et.al. They preferred not to use PhishTank, because it doesn't contain useful data. Besides, they decided to use Anti-Phishing Working Group reports, containing a lot of useful data. After that, the students evaluate their metrics, explained by several graphs.

Referring to these graphs, they had the following conclusions :

- China has more Internet users but USA is the most targeted by phishing attacks.
- Chile notifies the most phishing websites.
- Netherlands has almost the same rate of attacks as USA (that is surprising).
- GDP per country : Chile is outlined, but there is a correlation between GDP and normalised phishing attacks.

Finally, some appendix are enclosed, explaining the different metrics and containing an explanation of the concept of GDP.

## **2) Strengths**

This report is clear and some points are very developed. For instance, they wrote a complete definition of the security issue (phishing). Also they have tackle the problem very well.

A lot of metrics is considered in this report. Their description is clear and understandable. Then, there is a good description of tools and websites. The metrics chosen are well explained. The choice of graphs is an excellent idea, it is easy-to-read. Fortunately, the interpretation of their results is clear.

The explanation of the concept of GDP is very useful and clear. It is also an interesting point to use a purely financial metric and involve monetary aspects from the beginning. Afterall, the final result is about economics of security.

### **3) Major Issues**

One major issue is that Chile problem is mentioned but not explained, and another one is that the GDP not so well interpreted (because of the complexity of the concept?).

They haven't provide any technical solution to the problem. They have just provided some general suggestions but haven't mention any algorithm or protocol that might help the vendors or users to stop phishing.

### **4) Minor Issues**

A minor issue is the fact that some metrics are said "feasibles" but not used in the rest of the report. In addition, some descriptions are long and repetitive sometimes (description of metrics several time, long definition of the word "metric").

Another detail is the absence of cover sheet in the report, not so important but noticeable.

They paste the links in the middle of the report. It would be better to have put numbers [1][2]. in report and paste the links in the references.

They better have put an image in report showing the real example of phishing attack just in case the reader has no idea of phishing.