Review /Feedback on Group 12's Block 4 Assignment paper
By Group 1

Summary

The security issue addressed in this research paper are botnet infections. The dataset that is used for analysis is a log file containing communication from spam botnets. The paper aims to recognise and understand the factors that influence the variance in security performance in relation to metrics, and the different risk strategies that shape this variability. Odds Ratio and Pearson's Correlation functions have been used for statistical analysis of the data collected regarding the factors.

Three actors namely the National Cyber Security Center, the common internet user and Dutch ISP are taken into consideration to perform an analysis on countermeasures they can take against botnet infections. The costs, benefits and incentives involved, and the roles that externalities play in the security issue have been addressed for each actor.

Strengths

· Countermeasures have been identified and explained in detail for the first actor that was identified, that is the National Cyber Security Center.

· Along with the financial costs, non-financial costs also have been identified for the three selected actors, this gives a wholesome understanding of the costs.

· Factors that cause a variance in the metrics have been well recognised.

Minor Issues

· Grammatical errors and typos were identified, and the paper's author names are missing!

· No specific research question.

· System staying quick/available and investing time/effort to update (2.2.4) cannot be recognized as externalities in the right sense.

· There is no explanation for the conclusion reached regarding the GCI score in section 3.3.2, it only points to the findings of another paper.

· A lot of data outside of the recognised factors have been displayed in the table regarding botnet infections in various countries.

Major issues

· Although the paper claims that statistical analysis has been performed, Pearson correlation calculation has not been shown and explained explicitly. Thus the validity of the conclusions can be questioned – only the value of p has been mentioned.