Assignment Block 4 Group 7

Reviewed by group 1 27-10-2015

Summary

This paper analyzed three actors related to the security issue: governments, access providers and end users. It looked at the, countermeasures the actors could take, their incentives, externalities and cost/benefit distribution. The countermeasure the government can take it to create anti-botnet initiatives. Governments have a low incentive to do this. The access providers, ISPs and hosting providers, can disconnect an end user's device from the internet or choose not to host spam servers. End users can choose to install antivirus software, the incentives for the end user differs per person and relies on many factors.
Lastly, various factors were analyzed by correlating them to botnet infections. There is a positive correlation between internet subscribers and piracy rates. The factor of 'number of Internet subscribers' best explains the variance of the average number of bots per number of users.

Strengths of the assignment

- Clear structure of the paper.
- Proper and structured use of argumentation.
- Extensive analysis of the factors and their correlation to the security issue.

Major issues

Section: Introduction

- No major issues.

Section: Actors and their strategies for mitigation

- Government's botnet mitigation effort:
    - In the externalities section, a list of benefits is provided. But there are also some negative effects for externalities. For example, anti-botnet actions might cross paths with ongoing research by security companies.
- Access provider's mitigation effort:
    - Well written
- End user's mitigation effort:
    - I would say end users benefit from antivirus regarding botnets when the infection itself has other (often occurring) disadvantages. For example, if you're infected by financial malware (EG. the Zeus botnet you recalled), then criminals could also be tampering with your financial details / doing malicious transactions. Secondly, the way you phrase it, I'd indeed say end-users have very little incentive. In a way, they are their own externality, as most users will acquire antivirus for other end goals.

Section: Factors that explain differences in government's performance

- The statistical correlations are well done, however there no link to causal relations. Also it is not always clear how certain factors were quantified to calculate a correlation.

Section: Conclusion

- No major issues.

Minor issues

Section: Introduction

- Perhaps it is an idea to repeat what the metric is, given that you only have to analyze one in this paper. It may clarify things for readers who have not read the previous papers.

Section: Actors and their strategies for mitigation

- Government's botnet mitigation effort:
  - Typo in line two if section 'disincentives.'
  - Make sure to stay 'brief' when asked
- Access provider's mitigation effort:
  - It feels like the antivirus measure is a bit farfetched for ISPs to establish for end-users. It indeed fits best as a countermeasure for the last actor you discuss.
- End user's mitigation effort:
  - The incentives of the end user are also related to the mitigation efforts of other actors. For example, if ISPs decide to act against botnets, end users might be less inclined to. Also anti-virus will help against other infections and problems than only spam.

Section: Factors that explain differences in government's performance

- Piracy rates and Internet Subscribers:
  - How does the correlation between this relate back to the number of bots per million users?
- Rule of Law:
  - Which factor of the rule of law index did you use to calculate the correlation? The rule of law score consists of many factors, some have little correlation to the subject. You might want to reflect on a certain aspect such as 'Order and Security'.

Section: Conclusion

- No minor issues.