Assignment Block 2 Group 7

Reviewed by group 1 28-09-2015

Summary

This paper discusses the phenomenon 'botnet' with the help of a database provided by The Spamhaus Project. Ideal metrics have been described, for everything related to botnets, from the perspective of country-level decision makers, organizational-level decision makers and individual-level decision makers. Based on the dataset, two metrics have been chosen to further analyse: Bot distribution per country, and per AS. The evaluation shows that it is important to normalize the data and that few AS are responsible for most of the botnets.

Strengths of the assignment

- Decisions are well motivated
- There is a thorough analysis of the metrics and data
- Good use of external sources and data
- The data is well graphed and useful for further analysis

Major issues

Section: Project description

- This section misses a description of a general security issue you would like to analyse. The text does mention that you would like to look at botnets, however this is too general. The security issue then depends on the point of view: would you like to analyse it from the point of view of defenders or of attackers?

Section: Ideal metrics

- The descriptions of the metrics lack a motivation why this metric is ideal to analyse your security issue. Also, you distinguished between three levels of decision makers, but there is no motivation why this is correct or that this selection covers all decision makers.
- Some of your (ideal) metrics seem to have very little coverage of your (presumed) issue. Things like measuring mitigation efficiency are very hard on itself, but since you didn't formulate a clear issue, we can't provide proper feedback regarding the metrics you provide.

Section: Existing metrics

- It is not clear where this data is coming from. It is also not clear how these existing metrics relate back to your security issue. It now seems as if you have taken all metrics related to botnets used by companies, instead of focusing on one specific issue. In other words: why are these metrics ideal for to investigate your issue?

Section: Defined metrics

- Again this section does not explain why these metrics you chose relates back to the security issue. Also, from all the metrics in Table 2, why did you choose not to use certain metrics?

Section: Results & Evaluation of the Defined Metrics

- Metric 1
    - Number of bots: What does this data tell you? For example, what does it mean that India is ranked 17th after normalization, whereas it was second before?

Section: Evaluation

- How do your results bridge the gap between ideal metrics and existing metrics?

Minor issues

Section: Existing Metrics

- Table 2 - summary of existing Metrics on Botnet Measurement - the second column sometimes does not provide any information. An example is ‘Estimated number of bots’. Perhaps an explanation can be added as to why this is. Another point: What is CCM?

Section: Evaluation

- Don’t provide unnecessary information. In the result section you start off with the ‘number of bots per country’ metric. You normalize this in a latter stage, which is fine. But providing so much information and plotting the ‘unnormalized’ data seems a waste of your readers time. There is no real additional information here.