Economics of Cyber Security

Assignment Peer Review: Zeus and Feodo Tracker

by group 4

GROUP 5:
Raditya Arief
Eren Celik
Ana Guerra
Luigi Tuttobene

The assignment deals with Zeus botnet, a malware which is accountable for many financial frauds. Juxtaposed to other botnets, Zeus presents an atypical stealth ability, which make detection of the malware a such a hard task that often users find out to be infected only after an incident.

AV companies are the first identified actor. Their mission is to provide costumers reliable software in order to build consumer loyalty. At the same time they want to maximize their profit. They tend to use metrics based on vulnerabilities and incidents, and include the number of hashes and the detection ratio of competitor products. An ideal metric for AV providers.
Organizations might fall victim of botnet attacks. To avoid this scenario, they rely on metrics similar to the AV sellers, while ideally they would like to have control on the amount of employees who click suspicious links.
Also the police forces are seen as a security decision maker, as they go after the bad guys and try to limitate the spread of Zeus. Metrics for this actors involve the location of the server and ideally the amount of money stolen.
Banks are identified as actors too, since they covers damages.

Three metrics are then introduced, all based on TLD:
- Used Top Level Domains by Zeus
- Registrars used for Zeus C&C servers
- Hosting companies used for Zeus C&C servers

In the last part, these metrics are applied to a dataset, and result are graphically illustrated.
First, most part of top Zeus' TLDs are commercial domains (.com, .net) with the only exception of .ru. Second, it comes out that the highest percentage of the registrations is due to a small number of users.

In the first part, the topic is well introduced, explaining what Zeus is and how it operates.
The analysis of the security decision makers is pretty exhaustive (especially appropriate the paragraph on law enforcement) and the concluding table is a good way to summarize.

Major issues:
- unappropriated references: from the introductory explanation of Zeus to claims like "Zeus is widespread, with approximately 3.6 million infections in 2009 in the United States only. With this number, Zeus was the number one botnet in 2009." (pg 1) must be supported with references.
- Moreover, you must acknowledge all the sources for metrics that you report as "in practice".

Minor issues:
- An introduction to the paper, in which you state what you are going to do, why and how, will improve readability.
- Why what you indicate as "ideal metrics" are actually ideal? which is the impossibility in assessing them?
- When talking about metrics for the organization, you introduce "probability of infection (number of infected machines) - the probability of infection can be used for risk

assessments". Not clear why you write: "probability of infection (number of infected machines)".

- If you add a table, you are also supposed to explain its relevance in the text.
- A description of the dataset would help the reader follow your argumentation.
- The last section about evaluation could have been slightly richer, maybe adding some comments about your measurement or via comparison with average literature values.
- Few unappropriated lexical choices: some examples: "This server is managed by the person that manages the botnet"; "While Zeus can be used for many (malicious) objectives, it is mainly used for financial fraud." (should use concessive, not adverse conjunction);"software vendors of antivirus software are "responsible" for..."; "stealthing" pg 1.