Feedback from Group 5 to Group 7

Summary

Group 7 is analyzing ransomware, which is one of the popular topic in the cybersecurity world. Ransomware is an attack which the attackers locked down the victim data, which only able to be opened if the victim pays the attacker. The security issue is defined as "The exploitation of legitimate domain registrar services for ransomware hosting".

Group 7 is analyzing the dataset to be able to detect which domain registrar are more prone to ransomware, or furthermore take down the "dangerous" domain registrar. Some metrics on the dataset were analyzed to see whether there were a correlation between those metrics and the level of safety of the domains.

Weakness

1. Security Issue

- We are not sure if we can categorize this as a weakness, but we were a bit confused about the metrics derived from the dataset. Are they used to measure the security issue?, or are they used to measure something else to detect the security issue?
- The metrics did not show how they will measure "The exploitation of legitimate domain registrar services for ransomware hosting". The group defined measures regarding:
    - Threat removal effectiveness comparison among countries and worst effectiveness.
    - Ransomware detections per month
    - Domain registrars preferred for a particular ransomware

2. Structure

We feel that the paper is very lengthy and can be reduced, especially regarding some parts which are basically repetitions of study material that has been discussed in the video lectures on edX (the main culprit here being the "Security Metrics, explained" section). It is too long although it is nicely written.

3. Evaluation of Data sets

You proposed several example of metrics that can be used to measure the security issue, but as you explained there were several metrics which did not really correlate well to the issue, e.g. the country removal efficiency. It would be nice if in the conclusion you can also conclude which metrics that can really be used for your selected issue.

Strength

- A security issue is clearly defined.
- There is a methodology about the approach the group took to do the assignment.
- The document has a clear structure.
- Group mentions that they took perspective of the domain registrars.
- The use of extensive literatures.
- Found a lot of metrics existing in practice.