Group 6 - Malware/Virus Droppers

Rough summary

The security issue concerns the malicious usage of domain names. In this assignment, the authors look at the different registrars as the problem owner, rather than ICANN as the registers are in a better position to act. The problem is described from the perspective of multiple actors (ranging from the problem owner to attacker) and describes for each of them the most likely risk strategy. The authors finally choose to calculate the ROSI of a risk reduction strategy whereby the registrar monitors domains using an Intrusion Detection System to determine if it is malicious. Malicious domains are then taken down which would reduce the loss. It is then calculated that the proposed solution has a ROSI of 900%.

Strengths of the assignment

- Good introduction where the important parts of the previous assignment are repeated
- The reference to previous literature is nice as well
- For the different types risk strategies, several examples are given, including situations in which the strategy would likely be preferable
- Throughout the paper, the perspective of multiple actors is considered

Major issues

- Although it might be hard to give an accurate reference for the mentioned costs/benefits/risk mitigated, most of the numbers come without a rationale. Specifically, the damages per incident (e.g. malware domain) of 5000 seem quite high but without source it is hard to say if this is fair number.
- There is no loss distribution assumed, simply a constant number. Given the uncertain nature of the elements of ROSI, there is a large amount of uncertainty in loss and that should be expressed in the calculation and final ROSI

Minor issues

- In the Return on Security Investment it is mentioned that there are technical differences between just a hosting provider and one also providing hosting. There is no further mention if this difference also results in different costs or a different mitigation ratio.
- There is some discussion on the evolution of risk mitigation, but this is not specific to the described security issue
- As I haven’t read your first assignment, it would have been nice to see the results of your metrics for a point of reference, rather than referring to that assignment. Each assignment can then stand alone
- Referencing the foundation for categories of risk management strategy helps to add reputability to the system.