Peer Review for Group 9 on assignment Security Investments

By Group 13: Rob van Emous, Rien Heuver & Patrick van Looy

Summary

In the assignment, the group members continued on their last report in which they created and evaluated two security metrics with regard to antivirus companies (AVs). Their focus in this report is on possible security strategies the AVs could employ to reduce the security issues. First, they show how the security metric evaluation is related to the level of company security. Furthermore, they state the additional involved actors (users & cyber criminals), the risk strategies to reduce problems of the AVs (threat intelligence sharing & user awareness campaigns) and of the other actors (not download from or use certain websites & ISPs sharing threat intelligence). Then, they state the possible (financial) benefits to the actors of using these strategies. Finally, they calculate the Return On Security Investment (ROSI) for a client of an AV and conclude the report.

Strengths

- In general, it is a well structured report which includes all necessary information and is aided by some clear and helpful visualisations.
- In the introduction, they summarized the contents of the last report. This shows that this reports really builds on the previous work. It also quickly gets a reader which did not see the first report up to speed regarding the subject.
- In section 4.2 and 5.1, you have included the actors: ISPs and hosting providers in the evaluation of risk strategies and their benefits. These are important actors because they play a key role in protecting their network and informing users.
- In section 5.1, a very clear and detailed description of the AV company costs for executing the strategies is provided. We especially like that they take into account possible malware-discovery bounty programs and even discuss the matter on the level of printing and paper costs :). Well done!

Major issues

- In section 2, the relevant differences in security performance of the metric ‘VirusTotal Score’ is discussed, but the ‘Location based’ metric is neither discussed nor mentioned in this section. For completeness, they should either have included this metric as well or at least have explained why it was left out.
- In section 3, the actors influencing the security issue are described. Currently, only single users of the AV software and cyber criminals are listed. Although we agree that these actors are the most important ones, more actors should have been included and

some actors could have been split in multiple variations. For instance, users could have been split in educated and uneducated and/or personal users and companies. Also, ‘cyber criminals’ could be split based on the amount of resources and knowledge the criminal has (script kiddies vs state-funded hackers). As mentioned in the last bullet point of ‘Strengths’, you added two actors in later sections, but it would have been good to have introduced them first.

- Also in section 3, you claim that it depends on the users whether an AV company needs to review a website that is not in the malware domain list. However, proper AV programmes scan every website (known or unknown). Although, they might work with a default blacklist, the decision to mark a website malicious or not is not only based on the list. This would mean that an AV program is not able to detect new malicious websites, which is wrong. Knowing this, the users do not actually influence your metric.
- In section 4.1, again users are addressed, this time with awareness campaigns. However, in your reasoning, as a user of products from the AV company, I would say “Why would I buy your product, if I still need to check myself for malicious websites”. So either rewrite it more clearly, or remove this strategy (as currently, it is not that strong).
- In section 6, the ROSI is never actually calculated. So do I need to invest as a company, or not? This value is a major factor in choosing whether a security strategy is beneficial to a company and should have been included.

Minor issues

- General comment - Although the general quality of the individual sections is fine, the coherence of the report as a whole is lacking. We guess that this is caused by the group splitting the sections over the group members and not finalizing it by looking at the whole report. This last step is crucial in producing a consistent report.
- General comments - Instead of AV companies, try using terms that were in the lectures: Security provider/Security Industry. Also, use American notation for prices instead of Dutch (comma instead of dot) and do not use contractions (doesn’t, isn’t, etc.).
- In section 2, it is not described what the metric means if VirusTotal does not list a domain as malicious but an AV company does.
- In section 3, the number of websites on the internet is said to be increasing ‘ever since’ the 1-billion-sites mark was passed in 2014. However, from figure 2 we learn that the total number of websites has actually decreased in 2015 compared to 2014. So, the statement and the figure are inconsistent and it would be better if either of them would have been altered.
- In section 4.2, it would have been valuable to mention the option for an ISP to directly block malicious sites (since in many cases they are required to by law).
- In section 6, a new actor is introduced (enterprise organisation). Previously, this actor is not introduced or discussed.
- In the conclusion you state that costs vary immensely. Following, you give an example with only $13 difference. These two statements seems to be inconsistent and should have been altered.