Peer review to Group 6 – Reviewed by Group 11

- **A summary of the assignment:**
  The security issue focused on in their paper is, as stated in their paper, that of websites being used as an attack vector in a malicious campaign (p.1). They have therefore investigated a dataset containing a list of URLs, which have been detected to be malware or virus droppers. As the security issue can result in (reputational) damage for a registrar when an infected domain is removed by ICANN, the security issue is addressed from the viewpoint of the registrars. They explain that with "such a dataset" (p.3) it would be ideal to know exactly what malicious activity the URLs relate to. The metrics they have chosen are: Percent of infected TLDs vs. size of the TLD; Percent of infected TLDs vs. price of hosting a domain; and Total percent change in the proportion of infected domains. Their conclusions state (1) "Malware is at all corners of the internet. The measurements we have done show us that it is more common in some TLDs; (2) Malicious users opt to pay more for the hosting of their website on a smaller TLD, where the policies are not as strict or rules aren't administered so precisely; and (3) Malicious domains are generally decreasing showing registries and registrars are actively combating malware on their respective TLDs" (pp. 5-6).

- **Strengths of the assignment:**
  - In their paper the authors make the assumptions they made during their research explicit. For example, they state how they use the number of registered domains per TLD and pricing information in their metrics.
  - Clear explanation of the context of the study, for example section 2.1 and 2.2.
  - Results were clear, supported by comprehensible graphical representation.

- **The list of major issues:**
  - The structure of the paper is somewhat incoherent.
    - It is advised to explain your security issue and perspective in your introduction, so that the reader understands your angle earlier on. We thought your perspective was that of the registrars, but it is not very clear from both the introductory sections and the explanations of the metrics.
    - Now you explain your security issue after you have explained in detail your scope and context, and the associated assumptions you made regarding your dataset.
    - The dataset is discussed in the introduction, partly in section 3.2), and partly in section 4.3 ("The dataset's shear … month to month")?
    - You describe the security issue as 'websites being used as an attack vector in a malicious campaign' and 'state that to prevent such events from happening, multiple parties need methods in place to protect against malicious activity and remove malicious actors from their systems' (p.2). It is not clear which security issue will be examined.
  - It is not completely clear what the aim of your study actually is? Your defined metrics are explained and supported. However, because the unclarity of the security/aim of your metrics, it is not derived easily why it is useful to choose this metric.
  - In your section 4.1 and 4.2 you did not use any references. Why is it ideal "with such a dataset" (p.3)? Explanation of scientific metrics in practice or business metrics in practice is missing.
  - In your conclusion a recap on your research question (security issue and from what perspective you are addressing it) are missing.
  - Almost no use of references. A lot of statements with no scientific support. For example the metrics in practice.

- **The list of minor issues:**
  - The authors elaborate maybe too much on certain parts of the data in their explanation of the results, which goes out of the scope of their stated problem.
  - A tip is to add a correct reference list in APA-style. For example, reference 1 and 2 are missing hyperlinks for the reader to check on the data that the authors extracted from those sources.
  - “To analyze the dataset we have processed the data to extract “important” metrics, which will be explained later in the document” (p.1) -> What does ‘important’ metrics mean? For what is it important?
  - The paper includes a sweeping statement which looks incorrect. It's unclear if you could state that "...also each domain name registrars." (p. 1). Also on paragraph 2.2 you directly state that it is not each and every registrar.