Malware Analysis

Adrianna Holden-Gouveia
Website: `https://aholdengouveia.name`
in: aholdengouveia
: aholdengouveia
🐦: aholdengouveia

Objectives:

1. Understand the fundamentals of malware and viruses

2. Develop critical thinking skills in analyzing and mitigating malware threats

Answer the following questions

Malware and Virus Identification

1. Research and present summaries of two historical malware incidents (e.g., Stuxnet, WannaCry) that had a significant impact on security or society. Explain how these incidents occurred, their consequences, and the lessons learned.

2. Select a recent malware attack (preferably within the last 2-3 years) and provide an in-depth analysis. Include details such as the attack vector, the malware's behavior, the target(s), and the impact on affected individuals, organizations, or governments.

3. Discuss best practices and strategies for mitigating and preventing malware infections. Include information on antivirus software, network security measures, and user education. Explain how these measures can help protect against malware.

Reference information for CRAP/CRAAP

Turn in your report including your sources, you need at least 5, and a CRAP reliability checklist/paragraph for EACH source. CRAP or CRAAP is used to define the quality of your sources.

- You need at least 5 sources, and a CRAP reliability checklist/paragraph for EACH source.
- You may use either APA or MLA for your citations. If you want to use something else please just check with me first.
- Do not copy/paste from anywhere without citing your reference. Quoting or paraphrasing from a web site should include a citation.
- If you copy and paste into your paper, it is a quotation. It needs quotes and a link to the information (the link may be cut and paste from the address bar).
- If you use material that is only changed in minor ways (words or phrases omitted, shortened or slightly rearranged) it is a citation. It does not need quotes but does need a link to show from whence it came.
- If you take information from one source and substantially rephrase the material (paraphrase) it should be cited (show a link).
- Material drawn from multiple sources put in your own words does not need a direct citation but the sources would show up in any included bibliography.
- You can find instructions and more explanations for CRAP/CRAAP checklists at the following places
  - CRAP test explanation 1 `https://cccs.libguides.com/CRAPTest` or
  - CRAP test explanation 2 `https://libguides.butler.edu/c.php?g=117303&p=1940068`
  - Wikipedia explanation `https://en.wikipedia.org/wiki/CRAAP_test`

Deliverables

- The report should be at least three and a half pages not including citations, checklists, or anything besides actual content. Actual content should consist of:
  - 1 page for each Malware incident researched. Each page can include the link to the original article you used.
  - 1 page on the recent (last 2 years) Malware attack you've chosen.
  - 1/2 page on your recommendations for mitigation and why your suggestions are good ones.
- Please submit a word doc or PDF of your file.
- The report should include at least 5 references
- Your CRAP/CRAAP checklist for EACH of your 5 sources, but they should all be in the same document which can be different then the paper, or at the end of the paper