Exercise 1 (E1)

Attack Taxonomy and Cybercrime Organization

Part 2: ENISA Threat Landscape

Objectives

The objectives of part 2 of E1 are:

- To know about the ENISA Threat Landscape (ETL), an annual report on the status of the cybersecurity threat landscape. It identifies the top threats, major trends observed with respect to threats, threat actors and attack techniques, as well as impact and motivation analysis. It also describes relevant mitigation measures.
- To answer a set of questions about the newest ETL document (2024), and compare the answers with your findings in the exploratory research you did in the first part of E1.
- To compare 2023 edition with editions of previous years (2015, 2021), in order to find similarities and differences, as well as to draft a threat landscape evolution.

Statement

Download the **ETL 2024** document from the following link:

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Read the executive summary of the document in order to have an idea of its contents and main conclusions.

After that, generate a text document titled **E1_Part2**, and provide an answer to each of the following questions:

1) List the **prime threats** identified in the document. Compare this list with your previous exercise (E1 – Part1). Did you find them before? Are they appearing in your taxonomy?

2) Find in the document a definition of each of the prime threats. Discuss among you which definitions are close to your previous knowledge and which ones are introducing novel concepts and details.
3) Read about current **key trends** in the cyber threat landscape and identify examples of:
    a. Increasing trends
    b. Emergent trends
    c. Decreasing trends
4) Enumerate the main types of **cyber-threat actors** and define each of them. Explain whether you identified them in the first part of the exercise. Dive into the differences and similarities among them
    a. Are they targeting the same type of victims?
    b. Are they performing the same type of threats/attacks? Or in the same way (professionalization)
    c. Are their motivations similar? Specifically, are geo-political motivations equally relevant in all the cases?
5) Identify a threat actor that, although significant, is not included in the report as a prime threat actor, and answer why it is not included.
6) What is the ransomware group that performed a more consistent activity throughout the entire period of evaluation? Find information about this group in the report and complement it with external sources (who they are, structure, organization, motivation, etc).
7) Enumerate and briefly describe the top 3 well-known actors with most attributed threats/attacks in the reporting period. Search about all the information you can find about them in the document.
8) Let us know focus on the **Sectorial Analysis and Motivation.** Read those report sections and write a critical analysis of your findings, in order to answer:
    a. Why do you think public admin is the most targeted sector?
    b. What is the largest threat affecting individuals and why?
    c. Why ransomware is so spread among sectors?
9) Finally, let us focus on **Vulnerability analysis**. Review the contents of this section in order to answer the following questions:
    a. Explain what are the differences between Common Vulnerabilities and Exposures (CVE) system and Known Exploited Vulnerabilities (KEV) catalogue. How many new vulnerabilities have been identified in the reporting period? How many of them appear in either in CVE or in KEV or in both?
    b. Define what a CVE numbering organization (CNA) is and how many are identified in the document. Find the one that identified more critical vulnerabilities. Is there any CNA in Spain? If so, how many and enumerate one.
    c. Find and describe the top-3 weaknesses (regardless of its severity) and do the same with the top-3 weaknesses responsible of critical vulnerabilities. Are both lists different?
    d. What are the three major vendors that aggregate around 50% of all vulnerabilities that are routinely exploited?

After answering the questions before regarding ETL 2024, now read this short piece of news:

https://www.voanews.com/a/cyber-kidnapping-scams-target-chinese-students-around-the-world/7432998.html

10) Analyze the case from the main concepts you worked before: threat, actor, targeted sector, exploited vulnerabilities, weaknesses, impact, motivation. Is this case in line with the key trends of the current cyber-threat landscape?

Once ETL 2024 has been analyzed in detail, let us move back few years and compare it with previous versions published in 2015 and 2021:

ETL 2015: https://www.enisa.europa.eu/publications/etl2015

ETL 2021: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Take a look to the aforementioned documents and answer the following questions:

1) Compare the top/prime threats and sketch the evolution they suffered. Find examples of them that:
   a. Persisted active and important since 2015
   b. Their importance/prevalence declined with the years
   c. They recently appear or their importance/impact increased with the years.
2) Identify major differences in the social/economical/geo-political situation among years. Can you identify different events/situations that were important for the evolution of cyber-threat landscape?
3) Analyze and comment on the evolution of cryptojacking along the years

Delivery

Zip the document **E1_Part2** jointly with the document you prepared last week (**E1_Part1**) in a compressed file with name **E1_[your_team_number].zip**. Submit the file to **RACO (Practicals/E1**).

Aspects that will be positively evaluated during correction:

- **E1_Part1 (50%):** capacity of summarizing and processing information from different sources. Critical analysis on the provided contents (disparity among team members, if any, can be reported). Use of high impact sources (high-quality articles from well-known institutions/bodies). Clarity in the organization and presentation of the report.
- **E1_Part2 (50%):** accuracy and completeness of the answer to each question. Justify your answers when required. Critical thinking.

Deadline: October 10th, 23:59h CET

Supporting Material

ETL 2015: https://www.enisa.europa.eu/publications/etl2015

ETL 2021: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ETL 2024: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024