Security Lab – Analysis of the ETL Report

1 Introduction

ENISA[1] is the “European Union Agency for Network and Information Security”. It is a body of expertise, setup by the EU to carry out very specific technical, scientific tasks in the field of Information Security, working as a "European Agency". The Agency also assists the European Commission in the technical preparatory work for updating and developing Community legislation in the field of Network and Information Security. ENISA is helping the European Commission, the Member States and the business community to address, respond and especially to prevent Network and Information Security problems.

One of the more interesting products of ENISA is the annual *ENISA Threat Landscape Report (ETL)*. The reports can be found via the following link:

`https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends`

Note that the report usually covers a reporting period of about a year and summarizes the evolution of the threat landscape and observed trends during that period. The report is also available in the folder with the materials for this lab.

2 Task

The goal of this lab is to get a good impression of the current threat landscape as reported in the ENISA report and to critically assess the information contained in such reports. Note that the report also includes information that you will see or have seen in the lecture.

We recommend reading the entire report because it provides you with a good overview of the current situation. However, for this lab, you should first focus on chapters 1 and 2 and then read a selection (at least two) of the subsequent chapters on the prime threats (3 to 10).

Answer the following questions and send your answers (email or on paper) to the instructor:

- Why does ENISA release this report? What is the motivation?
- What is the target audience? There is information on this on at least two pages in the ETL report.
- What are supply-chain attacks and why are they not discussed in the report?
- According to the report, cybersecurity threats are on the rise. (This sentence has been in this lab since 2018, and it is as true now as it was then.) Which of the following statements are true according to the ENISA ETL? (These do change from year to year.)
  - □ The variety and number of observed attacks has increased
  - □ The number of ideologically motivated threat actors has increased
  - □ Ransomware attacks have increased
  - □ The impact of the attacks has increased
  - □ The overall number of threat actors has increased
- What was the main vector for ransomware delivery in 2023?
  - □ Human errors and system misconfiguration
  - □ Unpatched vulnerabilities in software and hardware
  - □ Phishing emails and brute-forcing of remote access credentials

[1] https://www.enisa.europa.eu/

  □ URL links and web browsing.

- What is the total number of incidents related to the prime threat categories in the ETL during the reporting period?
  - □ Approximately 200
  - □ Approximately 2’000
  - □ Approximately 20’000
  - □ Approximately 200’000
- Does the report identify sectors that were more affected by attacks than others? For example, in terms of the number of incidents?
- What do you think about characterizing the threat landscape mainly based on incidents that were publicly disclosed/discussed? List some pro and cons for this approach.
- What sources of information have been used to compile the report? To be able to answer this question, you need to consider the clarifications and explanations scattered throughout the report. Is there any information about how the sources of information the reference or use collected the threat-information themselves?
- Do you consider the source of information as trusted and free of conflicts of interest? Why?
- Study at least one of the threats listed in chapter 3 to 10
  - Study the threat in more detail and write down two trends or facts that you find surprising or especially relevant to home users. Make sure that you provide a concise explanation WHY you find this surprising or especially relevant.

Lab Points

For **2 Lab Points** you must document your answers and hand in your results to the instructor. Please be brief but use entire sentences, individual keywords won’t be accepted. You can hand in pdf or include your answers in the e-mail.

You get 2 points if you provide reasonable answers. Solutions that were obviously copied from others won’t give any points.

If you hand in your solution via e-mail, use „SecLab - ENISA - group X - name1 name2“ as the subject; corresponding to your group number and the names of the group members (max. 2).