**Part 2: ENISA Threat Landscape**

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

The main threats we can find in this document are: Ransomware, Malware, Social Engineering, Threats against data, Threats against availability (Denial of service & Internet threads), Information manipulation & interference and Supply chain attacks.

Yes. Some of them appear in our taxonomy of D1.

1. **Find in the document a definition of each of the prime threats. Discuss among which definitions are close to your previous knowledge and which ones are introducing novel concepts and details.**

* Ransomware

The definition is close to our previous knowledge of the attack.

* Malware

Here, the definition is also similar to the one we knew previously but it provides novel concepts like Firmware. They say that Malware is software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity or availability.

* Social Engineering

The definition is similar to our previous knowledge about this type of thread.

* Threats against data

Although we already knew this type of thread, the document highlights the difference between a Data breach and a Data leak that we didn’t know.

* Threats against availability: Denial of service

This definition does not add any detail that we already know.

* Threats against availability: Internet threads

This definition does not add any detail that we already know.

* Information manipulation

This definition introduces the concept of FIMI, which we weren’t familiar with.

* Supply chain attacks

This definition introduces the concept of supply chain attacks, which we were not previously aware of.

1. **Read about current key trends in the cyber threat landscape and identify examples of:**
   1. **Increasing trends**

**The impact on the cybersecurity threat landscape of AI Chatbots**.The rise of generative AI tools like ChatGPT, Microsoft Bing, and Google Bard is significantly impacting the cybersecurity threat landscape. The danger lies in the sensitive data that users share while interacting with these chatbots in work and daily life.  
  
Also the **manipulation of Information with AI** is a cause for concern.

**Increased Interest in Supply Chain Attacks**. Threat actors are increasingly targeting supply chains, especially by using employees as entry points.

**Larger and More Complex DDoS Attacks**. DDoS attacks are evolving in scale and complexity, now targeting mobile networks and IoT devices. These attacks are also being used strategically in conflicts, indicating their growing significance in the cyber threat landscape.

* 1. **Emergent trends**

**New Social Engineering Model**. A new approach in social engineering involves deceiving victims in the physical world.

**Extortion Only Techniques**. Cybercriminal organizations are increasingly relying on extortion methods, particularly double extortion, where data theft is integrated into the attack process. This trend indicates a shift towards more aggressive tactics to pressure victims for some financial gain.

* 1. **Decreasing trends**

**Classic Mobile Malware**. There is a steady decline in traditional mobile malware types, while adware remains prevalent in terms of occurrences. Despite the decline, spyware keeps being a significant threat to mobile devices. This indicates a shift of focus rather than a decrease in mobile threads.

1. **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**

The main cyber-threat actors are:

* **State-nexus threat groups**: They are state organizations that operate in an effective manner to attack other states or large organizations in order to complete their military, economic or espionage objectives.
* **Cybercriminals**: They are criminals who attack their targets (whether organizations or individuals) to steal information from them and make them pay for it.
* **Hackers-for-hire**: They are professional criminals like the state-nexus threat groups (they also can serve them), and are dedicated to breaking down barriers to gain access to the criminal market.
* **Hacktivists**: Its main objective is to manipulate governmental information to achieve changes in society. They are not as professionalized as the other groups.

* 1. **Are they targeting the same type of victims?** No, they aren’t. Hacktivists and state groups are usually targeting governments, while cybercriminals target all types of groups.
  2. **Are they performing the same type of threats/attacks? Or in the same way (professionalization)**

Hackers-for-hire can help state-nexus groups in some way in order to perform some attacks. They threaten or espionage governments to be stronger as a state. Hacktivists don’t look for money, as the other three do.

* 1. **Are their motivations similar? Specifically, are geo-political motivations equally relevant in all the cases?**

No. The geo-political motivations are more relevant for Hacktivists and State-nexus groups. The motivation for cybercriminals is basically money. State-nexus groups also have money as a motivation, but not the only one. Hackers-for-hire motivations are to professionalism the sector.

1. **Identify a threat actor not included in the report, and answer why this report is not including it.**

The insider threat actor. It is not included because there are very few public reports on them.

1. **What/who is Hive ransomware gang and what happened to it? Why do you think it is included in this report?**

It is a cybercriminal group. Investigators were able to get inside this group, inside its infrastructure. I think they are in the report as an example that it is possible to join a group to destroy it from the inside. (The members later can join another group.)

1. **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.**

The top three are:

1- **NoName**. They are a Russian Hacktivist group. They launched a project named DDOSIA, where volunteers were encouraged to download a bot that launched denial-of-service attacks.

2- **Lockbit** and 3- **Cl0p**. Both Lockbit and Cl0p are Ransomware related groups. Lockbit used to be the number 1 of them, although Cl0p is now. Their attacks included victim extortion, and they dominated (each one in a different period) the cybercrime landscape.

1. **Let us know focus on the Sectorial Analysis, Impact Assessment, and Motivation. Read those report sections and write a critical analysis of your findings, in order to answer:**
   1. **Why do you think public admin is the most targeted sector?**
   2. **What is the largest threat affecting individuals and why?**
   3. **Why ransomware is so spread among sectors?**
   4. **Order the impact (from largest to smallest) of supply chain attacks and interpret the results.**
2. There are five reasons why threat actors act. They are financial gain, espionage, disruption, destruction and ideology. As all of them can be related to public admin, it could be the reason why this sector is the most targeted one.
3. The largest threat affecting individuals are data-related threats. (Although social engineering and information manipulation have individuals as the most common target). The reason may be that individuals usually have no experience / knowledge in cyber security, so they are an easy target. Also, in the case of data-related threats, once the victim has been stolen, attackers have all the information to impersonate them, and it is difficult for companies to prevent that.
4. Malware is very popular because it is easy to use for attackers, and the attacks can be sent to different targets at the same time without much change to the way it works depending on the company or individual.
5. The ordered impact is: public administration (21%), digital service providers (16%), digital infrastructure (10%) and energy (9%). These attacks are more effective the more sensitive the information they handle, and the more targets they can affect at the same time. Public administration usually has sensitive information, and the other three are important in the operation of various industries at the same time.
6. **Finally, let us focus on Vulnerability analysis. Review the contents of this section in order to answer the following questions:**
   1. **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?**

Common Vulnerabilities and Exposures (CVE) is a standardized way for identifying and naming security vulnerabilities, CVEs are used to track and reference information about vulnerabilities, such as their severity levels, potential impact, and methods of mitigation. On the other hand, Known Exploited Vulnerabilities (KEV) is a list of vulnerabilities that meet three key criteria: must have a CVE ID, must have evidence of active exploitation by threat actors, and must have a clear remediation action.

During the reporting period, a total of 24.690 vulnerabilities have been reported (and assigned a CVE), and 100 of them are also present in the Known Exploited Vulnerabilities catalogue.

* 1. **Define what a CVE numbering organization (CNA) is and how many are identified in the document. Find the one that identified more critical vulnerabilities. Find information about Top-Level Root CNAs: what they are and how many are currently working. Is there any CAN in Spain? If so, how many and enumerate one.**

A CVE Numbering Authority (CNA) is an organization responsible for assigning CVE IDs to vulnerabilities and ensuring their accuracy and consistency. The document talks about a total of 49 CNA’s. mitre.org is the one that identified more critical vulnerabilities. Top-level Root CNA’s are numbering authorities that have a higher responsibility and manage other smaller CNA’s. In Spain we find the INCIBE (Instituto Nacional de Ciberseguridad), which is the only CNA of the country.

* 1. **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?**

Top 3 weaknesses:

1. **Cross-site Scripting (XSS)**: Improper Neutralisation of Input During Web Page Generation
2. **Out-of-bounds Write**
3. **SQL Injection**: Improper Neutralisation of Special Elements used in an SQL Command

Top-3 weaknesses responsible of critical vulnerabilities:

1. **SQL Injection**: Improper Neutralisation of Special Elements used in an SQL Command
2. **Out-of-bounds Write**
3. **Command Injection**: Improper Neutralisation of Special Elements used in a Command

Both lists are very similar except for one element. The elements that differ are Cross-site Scripting vs. Command Injection. This is because many webpages can be vulnerable to XSS attacks, so it is a very common weakness, but Command injection is much more severe and therefore it is found in more critical vulnerabilities.

* 1. **What are the three major vendors that aggregate around 50% of all vulnerabilities that are routinely exploited?**

The three vendors are *Microsoft*, *Apache* and *Fortinet* (tied in percentage with *SonicWALL*).

1. **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**

**Threat:** the main threat in this case is social engineering. It uses impersonation tactics usurping the mobile number of a victim’s contact to ask for money.

**Actor:** the actors might be cybercriminals that operate individually or for some organized group.

**Targeted Sector:**  the sector is targeted individuals.

**Exploited vulnerabilities:** this attack exploits social engineering by impersonating trusted contacts. Humans have a vulnerability in trusting relationships and emotional situations like urgencies.The actors take advantage of the weakness of the verification process that allows impersonation.

**Weaknesses:** the attack reveals weaknesses in the verifications processes of whatsapp. Additionally user’s lack of knowledge about this type of attacks increases susceptibility to social engineering scams.

**Impact:** the main impact is Economically because victims directly lose money through the fraudulent Bizum transfers. It also has a Social impact because it may cause a decrease of trust in digital communications. Psychologically victims may experience anxiety or confusion regarding their security.

Last but not least, WhatsApp could also suffer a reputational impact because of the negative publicity and users' distrust.

**Motivation:** the main motivation for the attackers is the financial gain. They exploit the trust of personal relationships to obtain quick money transfers.

This case aligns with key trends in the current cyber-threat landscape as it employs social engineering tactics. We have previously observed a rise in this type of attack.

**Once ETL 2023 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:**

| 2015 | 2021 | 2023 |
| --- | --- | --- |
| Malware  Web-based attacks  Botnets  Denial of Service  Physical threats  Insider threats  Phishing  Spam  … Ransomware (position 14) | Ransomware  Malware  Cryptojacking  E-mail related threats  Threats against data  Threats against availability and integrity  Disinformation – misinformation  Non-malicious threats | Ransomware  Malware  Social engineering  Threats against data  Denial of Service  Internet threats  Information manipulation and interference  Supply chain attacks |

* 1. **Persisted active and important since 2015**

The threat that has persisted more active and higher in the list since 2015 has been malware, followed by threats against availability such as Denial of Service attacks.

* 1. **Their importance/prevalence declined with the years**

Botnets have declined with the years, and also cryptojacking had a peak in 2021 but quickly declined too.

* 1. **They recently appear or their importance/impact increased with the years**

With the years Ransomware importance and impact has increased exponentially, mostly due to its financial viability and cybercriminal organizations that dedicate to it . Also supply chain attacks have increased lately.

1. **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?**

As it is commented in the 2021 report, COVID-19 and the digitalization of many operations drove cyber espionage tasking and created opportunities for cybercriminals. State-sponsored actors increased due to increased geopolitical tensions, and cybercriminal groups also increased due to the monetisation of activities such as ransomware attacks and extortion.

In the most recent years, geopolitical tensions are higher than ever with the conflicts taking place in Ukraine and Israel (and others), and cyber-warfare tactics are now more used than ever before, also due to the non-stopping rise of state-sponsored actors. Cybercrime organizations have also evolved, in some cases even hiding themselves behind “legitimate” businesses.

To sum up, the cyber-threat landscape has seen a “professionalization” process with the appearance of more organized cybercrime and the rise of state-sponsored groups.

1. **Analyze and comment on the evolution of cryptojacking along the years**

Cryptojacking has evolved significantly from its emergence in 2015 to 2023. In 2015, cryptojacking was not yet recognized as a notable threat and that's why it wasn’t featured in the Emerging Threats List (ETL) of 2015. However, by 2021, it surged in popularity, because of the rise of volatility of cryptocurrencies and the anonymity factor, making them increasingly attractive for cybercriminals.  
  
By 2023 the landscape of cryptojacking kept evolving as it continued to attract cybercriminals seeking reliable income streams. Some groups have shifted their focus from ransomware to cryptojacking, highlighting its ongoing profitability. This shift indicates that cryptojacking can offer a less obvious but still rewarding option for criminals.

However, this profitability comes at a time when law enforcement is paying closer attention to cryptocurrencies and enforcing stricter regulations. As authorities improve their ability to detect illegally obtained cryptocurrencies, cybercriminals are pushed to find new ways to carry out their attacks while facing stricter laws.