Question 1:

The ENISA Threat Landscape (ETL) report, now in its eleventh edition, plays a crucial role in understanding the current state of cybersecurity mainly within the European Union (EU). It provides valuable insights into emerging trends in terms of cybersecurity threats, threat actors' activities as well as vulnerabilities and cybersecurity incidents. Accordingly, the ETL aims at informing decisions, priorities and recommendations in the field of cybersecurity. It identifies the top threats and their particularities, threat actors' motivations and attack techniques, as well as provides a deep-dive insight on particular sectors along with a relevant impact analysis. The work has been supported by ENISA's ad hoc Working Group on Cybersecurity Threat Landscapes (CTL). In the latter part of 2022 and the first half of 2023, the cybersecurity landscape witnessed a significant increase in both the variety and quantity of cyberattacks and their consequences. The ongoing war of aggression against Ukraine continued to influence the landscape. Hacktivism has expanded with the emergence of new groups, while ransomware incidents surged in the first half of 2023 and showed no signs of slowing down. The prime threats identified and analysed include:

- Ransomware

- Malware

- Social engineering

- Threats against data

- Threats against availability: Denial of Service

- Threat against availability: Internet threats

- Information manipulation and interference

- Supply chain attacks For each of the identified threats, we determine impact, motivation, attack techniques, tactics and procedures to map relevant trends and propose targeted mitigation measures. During the reporting period, key findings include:

- DDoS and ransomware rank the highest among the prime threats, with social engineering, data related threats, information manipulation, supply chain, and malware following.

- A noticeable rise was observed in threat actors professionalizing their as-a-Service programs, employing novel tactics and alternative methods to infiltrate environments, pressure victims, and extort them, advancing their illicit enterprises.

• ETL 2023 identified public administration as the most targeted sector (~19%), followed by targeted individuals (~11%), health (~8%), digital infrastructure (~7%) and manufacturing, finance and transport. • Information manipulation has been as a key element of Russia's war of aggression against Ukraine has become prominent.

• State-nexus groups maintain a continued interest on dual-use tools (to remain undetected) and on trojanising known software packages. Cybercriminals increasingly target cloud infrastructures, have geopolitical motivations in 2023 and increased their extortion operations, not only via ransomware but also by directly targeting users.

• Social engineering attacks grew significantly in 2023 with Artificial Intelligence (AI) and new types of techniques emerging, but phishing still remains the top attack vector. The key findings and judgments in this assessment are based on multiple and publicly available resources which are provided in the references used for the development of this document. The report is mainly targeted at strategic decision-makers and policy-makers, while also being of interest to the technical cybersecurity community

PRIME THREATS A series of cyber threats emerged and materialised during the reporting period. According to the findings detailed in this report, the ENISA Threat Landscape 2023 report highlights and directs attention toward eight prime threat groups . These particular threat groups have been singled out due to their prominence over the years, their widespread occurrence and the significant impact resulting from the realisation of these threats.

• Ransomware

According to ENISA's Threat Landscape for Ransomware Attacks3 report, ransomware is defined as a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability. This action-agnostic definition is needed to cover the changing ransomware threat landscape, the prevalence of multiple extortion techniques and the various goals, other than solely financial gains, of the perpetrators. Ransomware has been, once again, one of the prime threats during the reporting period, with several high profile and highly publicised incidents.

• Malware

Malware, also referred to as malicious code and malicious logic, is an overarching term used to describe any software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity or availability of a system.

• Social Engineering

Social engineering encompasses a broad range of activities that attempt to exploit human error or human behaviour with the objective of gaining access to information or services. It uses various forms of manipulation to trick victims into making mistakes or handing over sensitive or secret information. Users may be lured to open documents, files or e-mails, to visit websites or to grant access to systems or services. Although the lures and tricks used may abuse technology, they rely on a human element to be successful. This threat canvas consists mainly of the following attack vectors: phishing, spear-phishing, whaling, smishing, vishing, watering hole attack, baiting, pretexting, quid pro quo, honeytraps and scareware. While social engineering techniques are often used to gain initial access, they may also be used at later stages in an incident or breach. Notable examples are business e-mail compromise (BEC), fraud, impersonation, counterfeit and, more recently, extortion.

• Threats against data

A data breach is defined in the GDPR as any breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed . Technically speaking, threats against data can be mainly classified as data breach or data leak. Though often used as interchangeably concepts, they entail fundamentally different concepts that mostly lie in how they happen4 5. Data breach is an intentional cyber-attack brought by a cybercriminal with the goal of gaining to unauthorised access and release sensitive, confidential or protected data. In other words, a data breach is a deliberate and forceful attack against a system or organisation with intention to steal data. Data leak is an event (e.g. misconfigurations, vulnerabilities or human errors) that can cause the unintentional loss or exposure of sensitive, confidential or protected data (intentional attacks are sometimes referred to as data exposure).

• Threats against availability:Denial of Service

Availability is the target of a plethora of threats and attacks, among which DDoS stands out. DDoS targets system and data availability and, though it is not a new threat, it plays a significant role in the cybersecurity threat landscape6 7. Attacks occur when users of a system or service are not able to access relevant data, services or other resources. This can be accomplished by exhausting the service and its resources or overloading the components of the network infrastructure8.

• Threats against availability: Internet threats

Threats to Internet availability refer to intentional or unintentional disruptions of Internet or electronic communications that result in Internet outages, blackouts, shutdowns or censorship. Internet disruptions can be due to government-directed Internet shutdowns, cyclones, massive earthquakes, power outages, cable cuts, cyberattacks, technical problems and military actions. These threats are diversifying and growing, having reached a new record in this reporting period and having caused huge monetary loss to national economies.

• Information Manipulation

Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. FIMI can be carried out by state or non-state actors, including their proxies inside and outside of their own territory, whereas in this report we study the threat regardless of its origin.

• Supply Chain Attacks

A supply chain attack targets the relationship between organisations and their suppliers9. For this ETL report we use the definition as stated in the ENISA Threat Landscape for Supply Chain Attacks10 in which an attack is considered to have a supply chain component when it consists of a combination of at least two attacks. For an attack to be classified as a supply chain attack, both the supplier and the customer have to be targets. SolarWinds was one of the first revelations of this kind of attack and showed the potential impact of supply chain attacks

It should be noted that the aforementioned threats involve categories and refer to collections of diverse types of threats that have been consolidated into the eight areas mentioned above. Each of the threat categories is further analysed in a dedicated chapter in this report, which elaborates on its particularities and provides more specific information on findings, trends, attack techniques and mitigation vectors. In the following figure it can be seen that ransomware and DDoS attacks were the most reported forms of attack during the reporting period and accounted for nearly half of the observed events followed by threats related to data. Moreover, we need to stress out that in several cases incidents involved more than one threat category and were thus analysed in the context of all respective categories. Given that the ETL is based on publicly available information and the fact that such information might not always provide the full picture, in certain cases incidents were not able to be classified into any threat category

RANSOMWARE

In ENISA's most recent report on the Threat Landscape for Ransomware Attacks312, ransomware was defined as: a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the assets' availability. This work covers the three key elements present in every ransomware attack:

- assets
- actions
- blackmail.

This action-agnostic definition was needed to cover the changing ransomware threat landscape, the prevalence of multiple extortion techniques and the various goals other than solely financial gains. This report also covers the four high-level actions (lock, encrypt, delete and steal) used by ransomware to impact the availability, confidentiality and integrity of the assets. It can serve as a reference to better understand this threat.

By contrast, the definition of ransomware in NIST describes ransomware as: a type of malicious attack where attackers encrypt an organisation's data and demand payment to restore access. In some instances, attackers may also steal an organisation's information and demand additional payment in return for not disclosing the information to authorities, competitors or the public313.

Once again, throughout the reporting period a substantial increase in ransomware-related incidents was witnessed, thus reaffirming the ongoing growth of the ransomware threat. Notably, the number of ransomware incidents has seen a noticeable surge, particularly since March 2023 . It is worth mentioning that the incidents under analysis predominantly centred on European Union (EU) countrie

LOCKBIT, ALPHV, AND BIAN LIAN STAND OUT AS THE TOP PERFORMERS, WHILE IN THE EU, PLAY GROUP JOINS THE RANKS OF LEADING THREAT ACTORS LockBit, ALPHV (BlackCat) and Bian Lian were some of the top ransomware strains used in RaaS (Ransomware as a Service) and extortion attacks in terms of victim organisations, dominating the Global landscape during the reporting period . Lockbit accounted for nearly half the number of incidents that were collected.

The sectors that are most frequently targeted by the top three ransomware groups encompass a wide range of industries, with particular emphasis on the Industrial and Manufacturing sector, which appears to have been the most frequently victimised during this reporting period. The reason the industrial and manufacturing sector stands out as the primary target for these top-tier ransomware groups could be because of its particular appeal to cybercriminals due to its heavy reliance on automation, supply chain operations and critical infrastructure.

Disrupting manufacturing processes or seizing control of industrial systems can result in significant financial losses and operational downtime, making it an attractive target. In the global landscape of ransomware incidents, it is evident that the United States emerges as the primary hotspot for cyberattacks, hosting a sizeable portion of the victims targeted by Lockbit.

During the reporting period, nearly half of all recorded ransomware incidents worldwide were concentrated in the United States The country's diverse range of industries, critical infrastructure and large corporations make it an attractive destination for cybercriminals seeking substantial ransoms.

RISE OF CLoP USE OF TWO 0-DAYS

In March 2023 (as seen in figure 22) Clop ransomware emerged as the dominant threat in the cybercriminal landscape, effectively dethroning the previous leader, LockBit. This seismic shift in the world of ransomware was primarily attributed to Clop's phenomenally successful GoAnywhere campaign. According to public reports, the group behind Clop managed to infiltrate and compromise a staggering 104 organisations during this period, and their ascent was fuelled by the exploitation of a critical zero-day vulnerability within the widely-used managed file transfer software, GoAnywhere MFT316. However, their audacious tactics did not stop there. On May 27th , a significant shift occurred in Clop's modus operandi when they began exploiting another vulnerability, identified as CVE-2023-34362, within the file transfer service MOVEit Transfer.

This timing was strategically chosen during the extended US Memorial Day holiday317 318, a period when many organisations have reduced staff and heightened vulnerabilities. It is worth noting that conducting cyberattacks around holidays has become a signature tactic for the Clop ransomware operation, as they have previously executed large-scale exploitation attacks during similar periods of reduced security staffing. The bulk of these MOVEit Transfer breaches appear to have taken place between May 30 and May 31. As a result of this Memorial Day attack on vulnerable internet-facing MOVEit Transfer installations, the number of alleged victims affected by Clop's ransomware campaign had exceeded an alarming count of 420319 by the conclusion of the reporting period.

It is worth noting that in both cases these campaigns did not involve any ransomware attacks, no ransomware was deployed, even though Clop is considered a ransomware group. This was a case of data exfiltration and extortion rather a trend, as seen below, is increasing.

This series of high-impact attacks showcased Clop's evolving and advanced capabilities, underscoring the urgent need for organisations to bolster their cybersecurity measures and stay vigilant against emerging threats in the everchanging landscape of cybercrime. The increased exploitation of two highly effective zero-day vulnerabilities has underscored the importance of responsible disclosure of vulnerabilities even further.

NEW TECHIQUES EMERGING

Franken Ransomware – code being repurposed

A noteworthy shift in the ransomware landscape has been observed from RaaS (Ransomware as a Service) towards independent actors. This intriguing development has given rise to a new phenomenon that has been coined as ‘Franken-ransomware’. This term aptly describes a trend wherein malicious actors are piecing together new ransomware variants using fragments of stolen or leaked code from various sources326. The ESXiArgs malware being used to target VMware systems starting in February was one such example, borrowing a ‘ransom note from one ransomware, the encryption scheme from another ransomware’ (potential Babuk).

Other emerging actors who have adopted this strategy include Rapture, which seems to have incorporated the leaked source code of the Paradise crypto-locker from 2021. GazProm, named after the Russian gas giant and known for its ransom notes featuring ASCII art of Russia's president, has used the leaked Conti source code. Additionally, newcomers such as the RA Group, Rorschach and RTM Locker have all integrated source code from the Babuk ransomware, which became available in September 2021327.

URL delivered Ransomware dominates attack vectors

Threat actors have adopted increasingly dynamic tactics for disseminating ransomware. Alongside the conventional use of polymorphic ransomware variants, they frequently alter hostnames, paths, filenames or a combination of these elements to broadly propagate ransomware. Historically, email attachments, such as those using SMTP and POP3 protocols, were the predominant means for distributing ransomware. However, recent findings from Palo Alto's Unit 42, who analysed ransomware samples throughout the whole of 2022, indicate a notable shift in the primary entry point for ransomware infections. URL links and web browsing have emerged as the dominant methods for delivering ransomware, accounting for more than 77% of cases.

Question2:

practices for securing personal computers:

A personal computer used without proper security measure could lead to exploiting the system for illegal activities using the resources of such insecured computers. These exploiters could be Virus, Trojans, Keyloggers and sometimes real hackers. This may result in data theft, data loss, personal information disclosure, stealing of credentials like passwords etc. So, protect and secure your Personal Computer before it is compromised.

Always install Licensed Software so that you have regular updates of your Operating system and Applications. In case of open source software, make sure to update frequently.

Read the “Terms and Conditions” / “License Agreement” provided by vendor/software before installation.

Properly shutdown and switch off your personal computer after the use along with your external devices like Monitor, Modem, Speakers etc.

Software Installation q

Installation of Operating System

Get proper Licensed Operating System and read License agreement carefully before installing the OS.

Switch on your personal computer and go to BIOS Settings and change your first boot drive to CD Drive.

Insert your CD/DVD into the CD drive and restart your system using Ctrl+Alt+Delete.

After restart, the system boots from the CD/DVD.

Follow the installation steps as specified by the vendor document.

Use the CD provided by the Vendor to install your w Motherboard drivers , Monitor drivers ,Audio & Video drivers ,Network drivers.

Physical Security

Regularly clean your system and it's components.

Properly organize the power cables, wires, to prevent from water, insects etc.

While working at PC, be careful not to spill water or food items on it.

Always follow "Safely Remove" option provided by the Operating System while disconnecting the USB devices.

By setting BIOS password, you can prevent unauthorized access to your personal computer.

Switch off the computer when it's not in use.

Note: To setup BIOS password refer "Setting password to BIOS" section.

Note: Turn your PC Off before cleaning it.

Data Security :

Enable Auto-updates of your Operating System and update it regularly.

Download Anti-Virus Software from a Trusted Website and Install. Make sure it automatically gets updated with latest virus signatures.

Download Anti-Spyware Software from a Trusted Website and Install. Make sure it automatically updates with latest definitions.

Use "Encryption" to secure your valuable Information. Note: For encryption password is required, always remember the password used while encrypting it, else data would not be available thereafter.

Strong password should be used for "Admin" Account on computer and for other important applications like E-mail client, Financial Applications (accounting etc).

Backup :

Periodically backup your computer data on CD / DVD or USB drive etc.. in case it may get corrupted due to HardDisk failures or when reinstalling/format ting the system. Browser Security: q Always update your Web Browser with latest patches.

Use privacy or security settings which are inbuilt in the browser. Also use content filtering software. Always have Safe Search "ON" in Search Engine.

Always use Anti-Spyware Software to scan the eMails for Spam. Always scan the e-Mail attachments with latest updated Anti-Virus and Anti-Spy ware before opening.

Always remember to empty the Spam folder. q Startup programs should be monitored / controlled for optimal system performance.

Recovery Disk:

Always keep recovery disk suplied by Manufacturer / Vendor of the Computer System to recover the Operating System in the event of boot fail- ures due to system changes such as uncerificated Drivers/unknown Software pub- lisher.

Browser Security:

Always update your Web Browser with latest patches.

Use privacy or security settings which are inbuilt in the browser.

Also use content filtering software. Always have Safe Search "ON" in Search Engine.

Internet Security:

Follow Internet Ethics while browsing.

Check the copyright issues before using the content of Internet.

Always access the site which uses https (Hyper Text Transfer Protocol Secure) while performing Online transactions, Downloads etc, which is secure.

If the site uses SSL, verify the Certificate details like Who is the owner, Expiry date of the certificate etc to confirm whether it is trusted or not. You can do this by clicking the lock icon.

Use only Original Websites for downloading the files rather than Third Party websites.

Scan the downloaded files with an updated Anti-Virus Software before using it. Install and properly configure a Software firewall, to protect against malicious traffic.

e-Mail Security:

Always use strong password for your email account.

Always use Anti-Spyware Software to scan the eMails for Spam.

Always scan the e-Mail attachments with latest updated Anti-Virus and Anti-Spy ware before opening. Always remember to empty the Spam folder.

Wireless Security:

Change default Administrator passwords.

Turn On WPA (Wi-Fi Protected Access) / WEP Encryption. Change default SSID.

Enable MAC address filtering. Turn off your wireless network when not in use.

Modem Security:

Change the default passwords.

Switch off when not in use.

Do's:

Read the vendor document carefully and follow the guidelines to know how to setup the personal computer Connect

i. Keyboard

ii. Mouse

iii. Monitor

iv. Speakers and

v. Network Cable …… to CPU (Central Processing Unit) as directed in vendor document. Connect CPU and Monitor to Electrical Outlets.

Dont's:

Do not install pirated software such as w Operating System Software (Windows, Unix, etc..).

Application Software (Office, Database..etc). w Security Software (Antivirus, Antispyware..etc).

Note: Remember, some Pirated Software themselve can be rogue programs.

Do not plug the computer directly to the wall outlet as power surges may destroy computer. Instead use a genuine surge protector to plug a computer.

Don't eat food or drink around the PC. Don't place any magnets near the PC.

Never spray or squirt any liquid onto any computer component. If a spray is needed, spray the liquid onto a cloth and then use that cloth to rub down the component.

Don't open the e-Mail attachments which have double extensio