DICYSTECH

DIGITAL TRAINING FOR CYBERSECURITY STUDENTS IN INDUSTRIAL FIELDS

www.dicystech.eu

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. «DICYSTECH - Digital Training for Cybersecurity Students in Industrial Fields» project number: 2020-1-ES01-KA226-HE-095291.

UPDATED CONTEXT OF THE PROJECT: THE INDUSTRY 4.0 CYBERSECURITY REALITIES AND NEEDS

Co-funded by the
Erasmus+ Programme
of the European Union

DICYSTECH

The European Union Agency for Cybersecurity - ENISA published the 9th edition of the **Threat Landscape 2021 (ETL) report**, an annual report regarding the status of the cybersecurity threat landscape "*that identifies prime threats, major trends observed with respect to threats, threat actors and attack techniques, and also describes relevant mitigation measures*".

Co-funded by the
Erasmus+ Programme
of the European Union

DICYSTECH

"*Cybersecurity attacks have continued* ***to increase through the years 2020 and 2021****, not only in terms of* ***vectors and numbers*** *but also in terms of their* ***impact***".

"*The* ***COVID-19 pandemic*** *has also –expectedly– had an impact on the cybersecurity threat landscape*".

"*The cybersecurity landscape has grown in terms* ***of sophistication of attacks, their complexity and their impact***".

"*The threat to supply chains and their significance due to their potentially catastrophic cascading effects has reached the highest position among major threats*".

Co-funded by the
Erasmus+ Programme
of the European Union

DICYSTECH

While in the previous edition….

Co-funded by the Erasmus+ Programme of the European Union

DICYSTECH

This year, ENISA took a step back and **consolidated threat categories in a move towards integration and better representation of similar threats.**

Co-funded by the Erasmus+ Programme of the European Union

DICYSTECH

ENISA also identified the **key trends** observed in the cyber threat landscape during the reporting period such as:

- **Highly sophisticated and impactful supply chain compromises** proliferated, as highlighted by the dedicated ENISA Threat Landscape on Supply Chain. **Managed service providers** are high-value targets for cybercriminals.
- **COVID-19 drove cyber espionage** tasking and created **opportunities for cybercriminals**.
- **Governmental organisations have stepped up their game** at both national and international level. Increased efforts have been observed from governments to disrupt and take legal action against state-sponsored threat actors.
- **Cybercriminals are increasingly motivated by monetisation** of their activities, e.g. ransomware. **Cryptocurrency** remains the most common pay-out method for threat actors.
- Cybercrime attacks **increasingly target and impact critical infrastructure**.
- **Compromise through phishing e-mails, and brute-forcing on Remote Desktop Services (RDP)** remain the two most common **ransomware infection vectors**.
- The focus on **Ransomware as a Service (RaaS) type business models** has increased over 2021, making proper attribution of individual threat actors difficult.
- The occurrence of **triple extortion ransomware** schemes increased strongly over the course of 2021.

Co-funded by the Erasmus+ Programme of the European Union

DICYSTECH

- **The malware decline** that was observed in 2020 continues during 2021. In 2021, we saw an increase in threat actors resorting to relatively new or uncommon programming languages to port their code.
- **Malware targeting container environments** have become much more prevalent, with novel evolutions like file-less malware being executed from memory.
- Malware developers keep finding ways to **make reverse engineering and dynamic analysis harder**.
- The volume of **cryptojacking infections** attained a **record high** in the first quarter of 2021, compared to the last few years. The **financial gain** associated with cryptojacking incentivised the threat actors to carry out these attacks.
- **The volume of Crypto mining in 2021 and cryptojacking activities are at a record high**.
- We can see that a **shift from browser to file-based cryptojacking** is taking place.
- **COVID-19 is still the dominant lure in campaigns** for e-mail attacks.
- **Business E-mail Compromise (BEC)** has **increased**, has grown in **sophistication** and become more **targeted**.
- **The Phishing-as-a-Service (PhaaS)** business model is gaining prevalence.
- Threat actors shifted their attention towards **vaccine information** in the context of threats to data and information.

- There was a **surge in healthcare sector related data breaches**.
- Traditional DDoS (Distributed Denial of Service) attacks are moving towards **mobile networks and IoT (Internet of Things)**.
- **Ransom Denial of Service (RDoS)** is the new frontier of denial of service attacks.
- **Sharing of resources in virtualised environments** acts as an amplifier of DDoS attacks.
- **DDoS campaigns** in 2021 have become more targeted and much more persistent and increasingly multivector.
- **Artificial Intelligence (AI)-enabled disinformation** supports attackers in carrying out their attacks.
- **Phishing is at the heart of disinformation attacks** and strongly exploits people's beliefs.
- **Misinformation and disinformation** are at the core of cybercrime activities and is increasing at an unprecedented rate.
- **Disinformation-as-a-Service (DaaS) business model** has grown significantly, spurred by the increasing impact of the COVID-19 pandemic and the need to have more information.
- In 2020 and 2021, we observed a **spike in non-malicious incidents**, as the COVID-19 pandemic became a multiplier for **human errors** and **system misconfigurations**, up to the point that most of the breaches in 2020 were caused by errors.
- There has been a **spike in cloud security non-malicious incidents**.

Co-funded by the Erasmus+ Programme of the European Union

In February 2022, **ENISA** and **CERT-EU** strongly encouraged all public and private sector organisations in the EU to adopt a minimum set of cybersecurity best practices.

Co-funded by the
Erasmus+ Programme
of the European Union

DICYSTECH

14 best practices suggested:

1. Ensure remotely accessible services require multi-factor authentication (MFA)
2. Ensure users do not re-use passwords, encourage users to use Multiple Factor Authentication (MFA) whenever supported by an application (on social media for instance)
3. Ensure all software is up-to-date
4. Tightly control third party access to your internal networks and systems
5. Pay special attention to hardening your cloud environments
6. Review your data backup strategy
7. Change all default credentials
8. Employ appropriate network segmentation
9. Conduct regular training
10. Create a resilient email security environment
11. Organise regular cyber awareness events
12. Protect your web assets from denial-of-service attacks
13. Block or severely limit internet access for servers
14. Make sure you have the procedures to reach out and swiftly communicate with your CSIRT

Co-funded by the Erasmus+ Programme of the European Union

DICYSTECH

DICYSTECH

CONTACT US

Coordinator: Anabel Menica TXORRIERI
amenica@txorierri.net

www.dicystech.eu

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. «DICYSTECH - Digital Training for Cybersecurity Students in Industrial Fields» project number: 2020-1-ES01-KA226-HE-095291.