EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA'S THREAT LANDSCAPE 2023

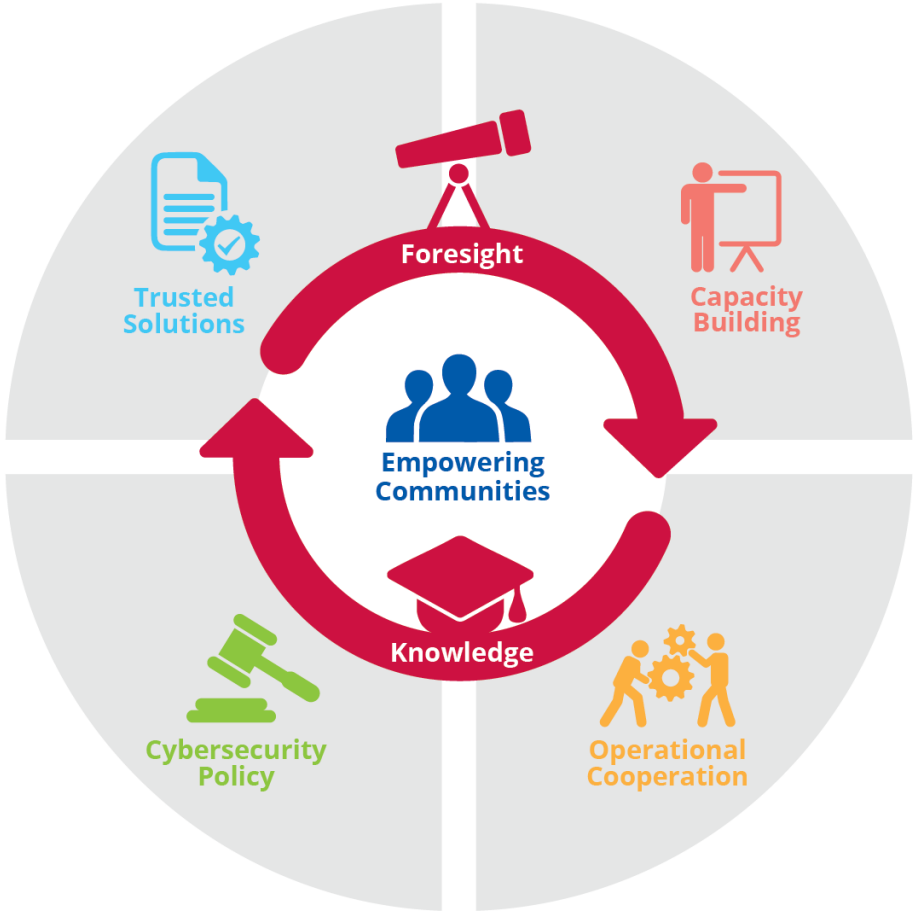
Ifigeneia Lella, Cyber Security Expert
ENISA

27 | 03 | 2024

ROLE OF ENISA – WHO WE ARE

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY



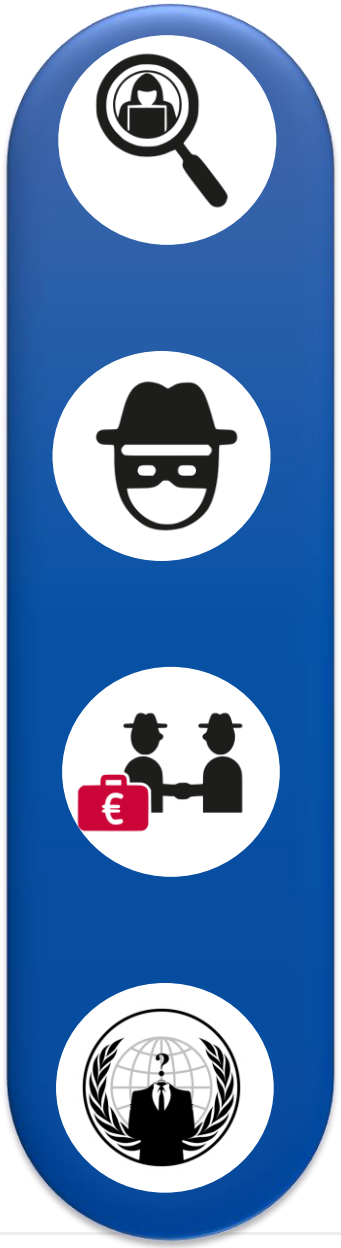
A TRUSTED AND CYBER SECURE EUROPE

Our mission is to achieve **a high common level of cybersecurity** across the Union in cooperation with the wider community

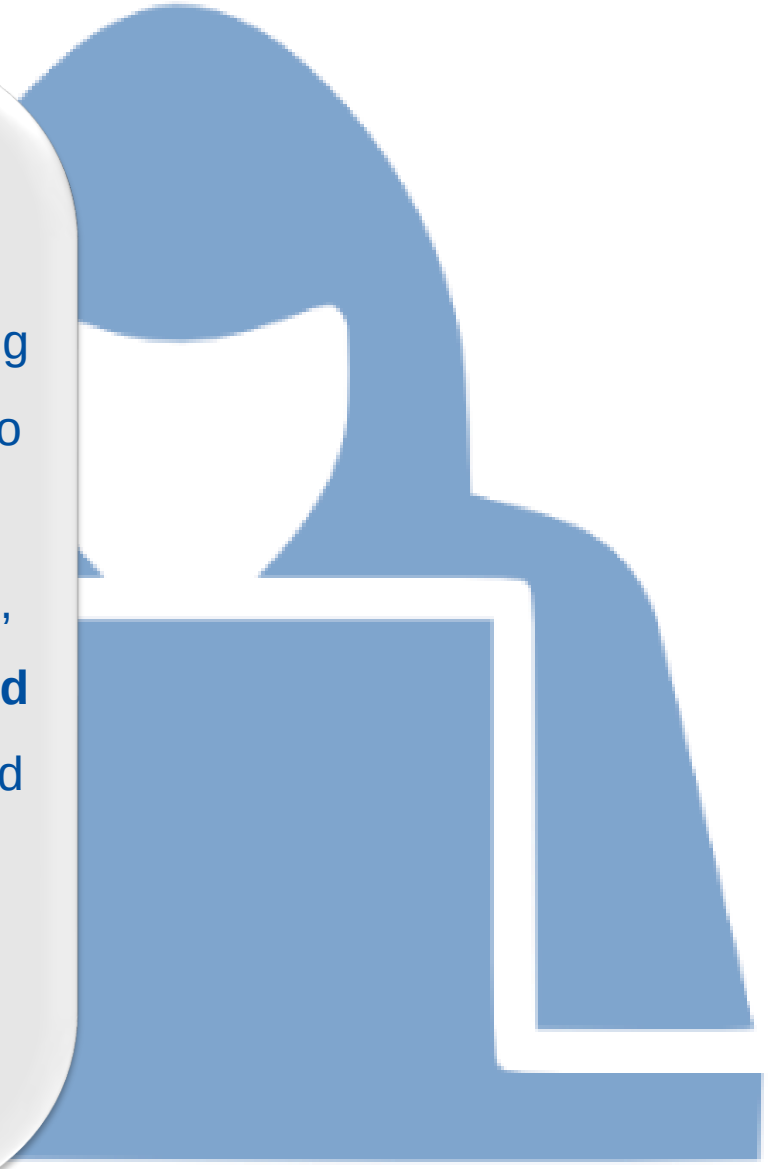
ENISA THREAT LANDSCAPE TRADITION

It's reflecting on the PAST to prepare for the FUTURE

THREAT ACTORS



- **Integral** part of overall threat assessment
- **Entities** aiming to carry out **a malicious act** by taking advantage of existing **vulnerab**ilities with the intent to harm their victims
- **Understanding how threat actors** (trends, targets , techniques, tools and procedures) **think and act and their motivations and goals** are essential for a good cyber security strategy



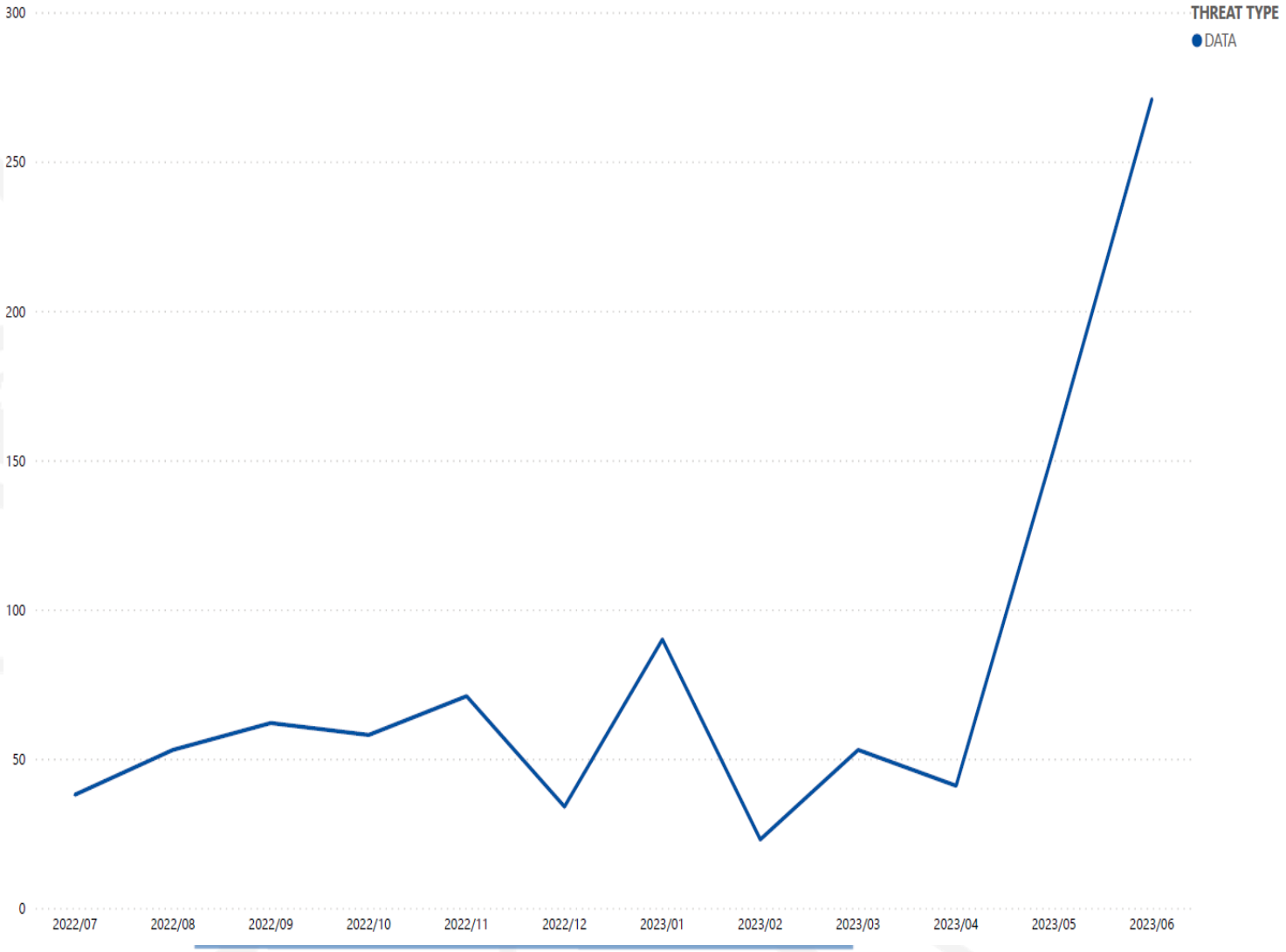
•Rising focus on edge devices.
•State-nexus groups exploit both old vulnerabilities and zero-days.
•Financial objectives tied with state-affiliated activities.

- valid accounts for initial access
- keep relying on Living Off the Land Binaries (LOLBins),
- continue to use cloud infrastructure.
- Old tricks remain a guarantee for success (SEO poisoning and malvertising)
- Deepfakes and AI

•The Initial Access Broker (IAB) market is expanding rapidly.
•Main product of IAB is credentials for VPN and RDP breaches.
•Attackers now favor adaptable and fast-changing methods.
•Cybercrime has become an organized sector with expert services.
•Many threat actors have enhanced their "As-a-Service" models.


Threats against data
Social Engineering threats
FAKE
ENISA
THREAT
LANDSCAPE

DATA THREATS



- **Increase in 2023**
- **Lack of transparency in data breach notices**
- **Cloud computing**
- **AI chatbots**

SOCIAL ENGINEERING THREATS

- **Phishing as the initial infection vector and on the rise**
- **Use of AI**
- **ABUSING MULTI-FACTOR AUTHENTICATION**
- **Re-emergence of call-back phishing**

RANSOMWARE

- March 2023 broke ransomware attack records - ransomware continues to be on the rise
- URL delivered ransomware dominates attack vectors
- shifting from encryption to data extortion

MALWARE

- Information stealers
- Evolution of malware delivery
- Mobile malware and spyware
- Installed malware

FIMI

- **Surge in Info Manipulation:**
- **Strategic Phases**
- **Geopolitical Influence:**
- **Cybersecurity Narrative**
- **Hacktivism**
- **Digital Presence & Masquerading: AI and Disinformation**

•Disinformation-as-a-Service
•Election Interference
•Revenue Generation: International Countermeasures

SUMMARY

Threat actors use whatever is more relevant and evolve and adapt to the changing of technologies

Good practices and coordinated actions are important to reach a common high level of cybersecurity.

Cyber attacks has increased by a lot compared to last year but we still lack the visibility

Information Sharing is caring…

It helps potential victims , it helps researchers.. it also helps cybersecurity authorities and ENISA

THANK YOU FOR YOUR ATTENTION

Agamemnonos 14, Chalandri 15231
Attiki, Greece

info@enisa.europa.eu

www.enisa.europa.eu