



# MONITORING THREATS TO TRANSPORT

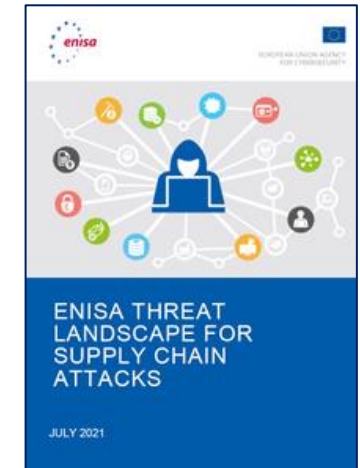
## Transport Threat Landscape

- Released: March 2023
- January 2021 to October 2022

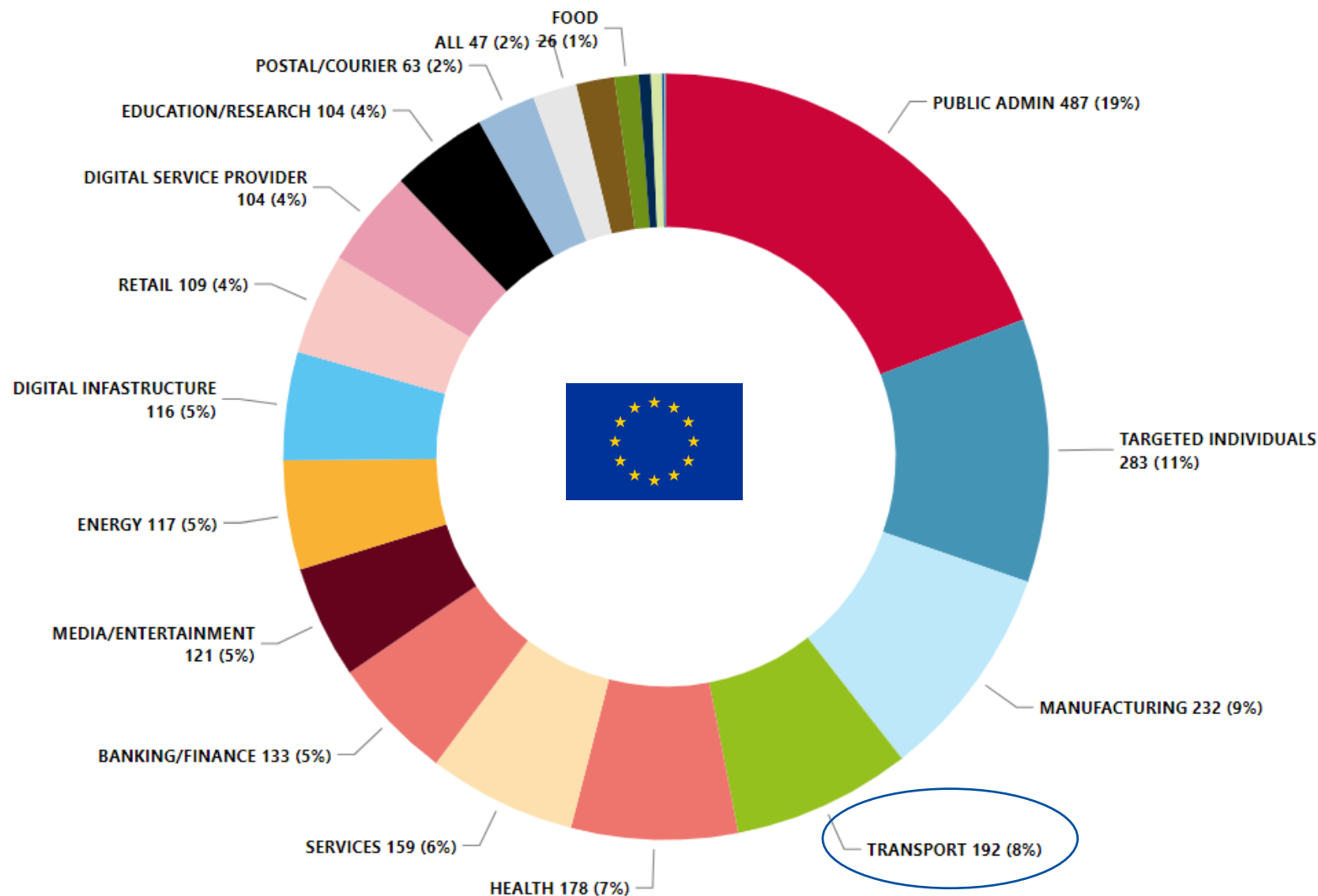


## 2023 Threat landscape (all sectors)

Upcoming in 2023: Report on DoS Attacks

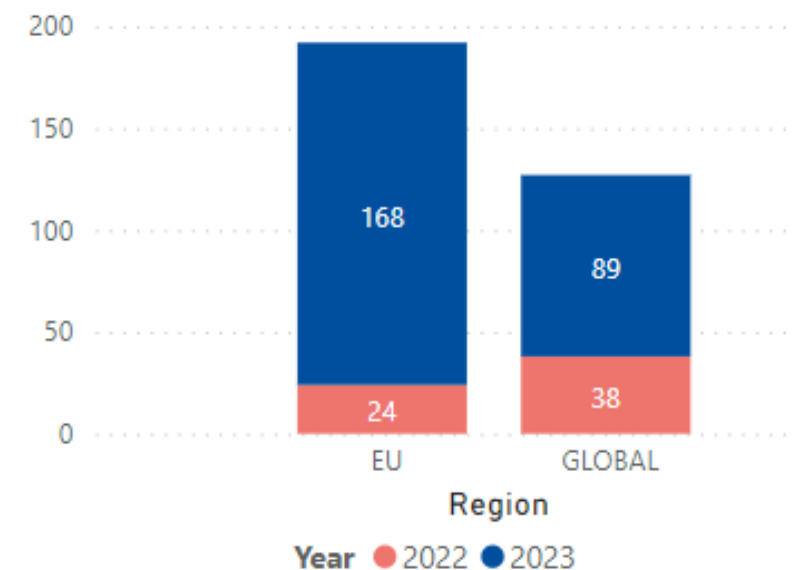


# 2023 THREAT LANDSCAPE (UPDATE)



## Sample:

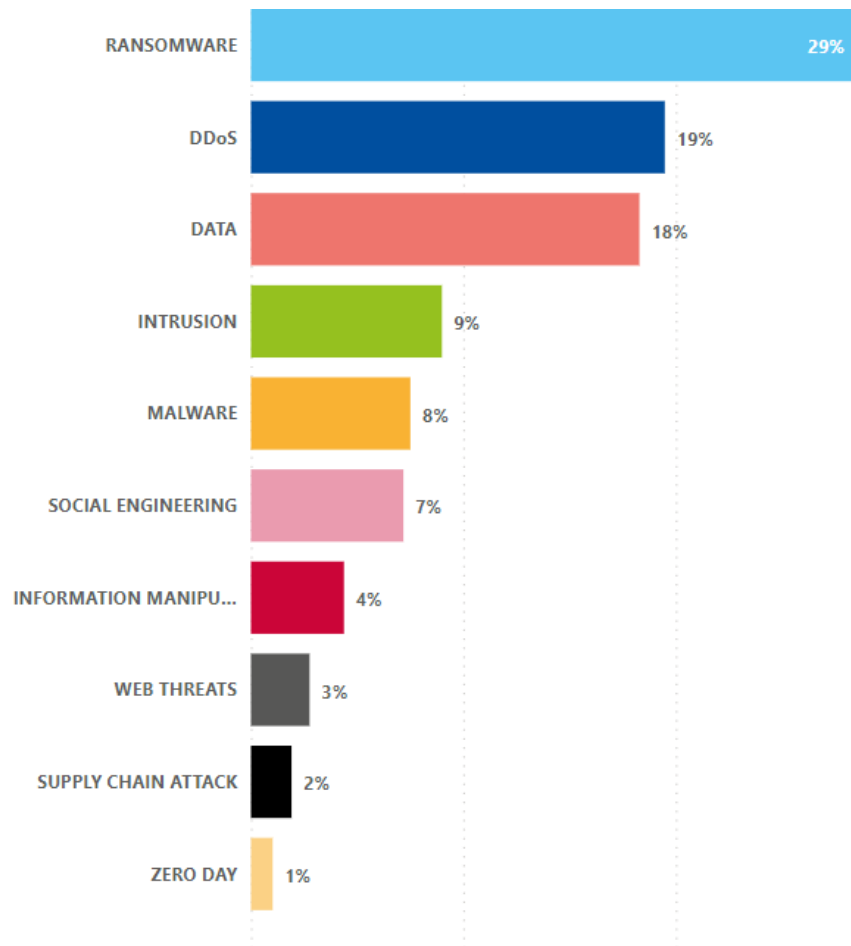
- **July 2022 to June 2023**
- **2580 incidents**, with an additional 220 incidents affecting more than one EU MS
- **192 incidents** affecting the transport sector in the EU



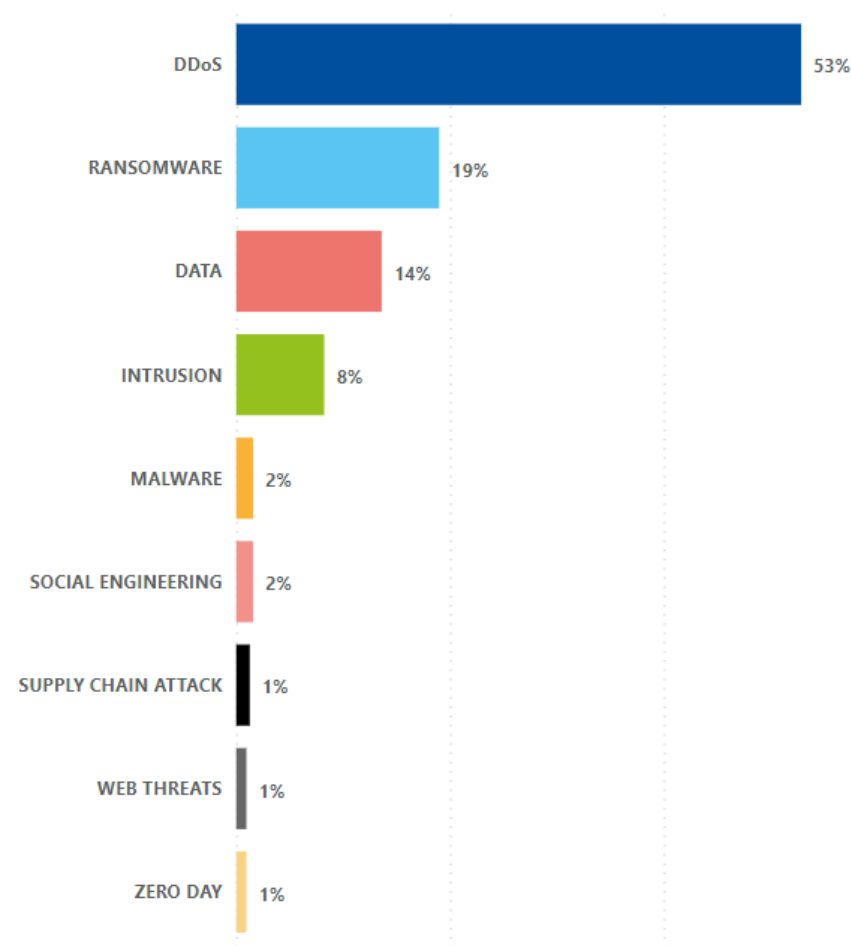
# PRIME THREATS IN THE EU (JULY 2022 TO JUNE 2023)



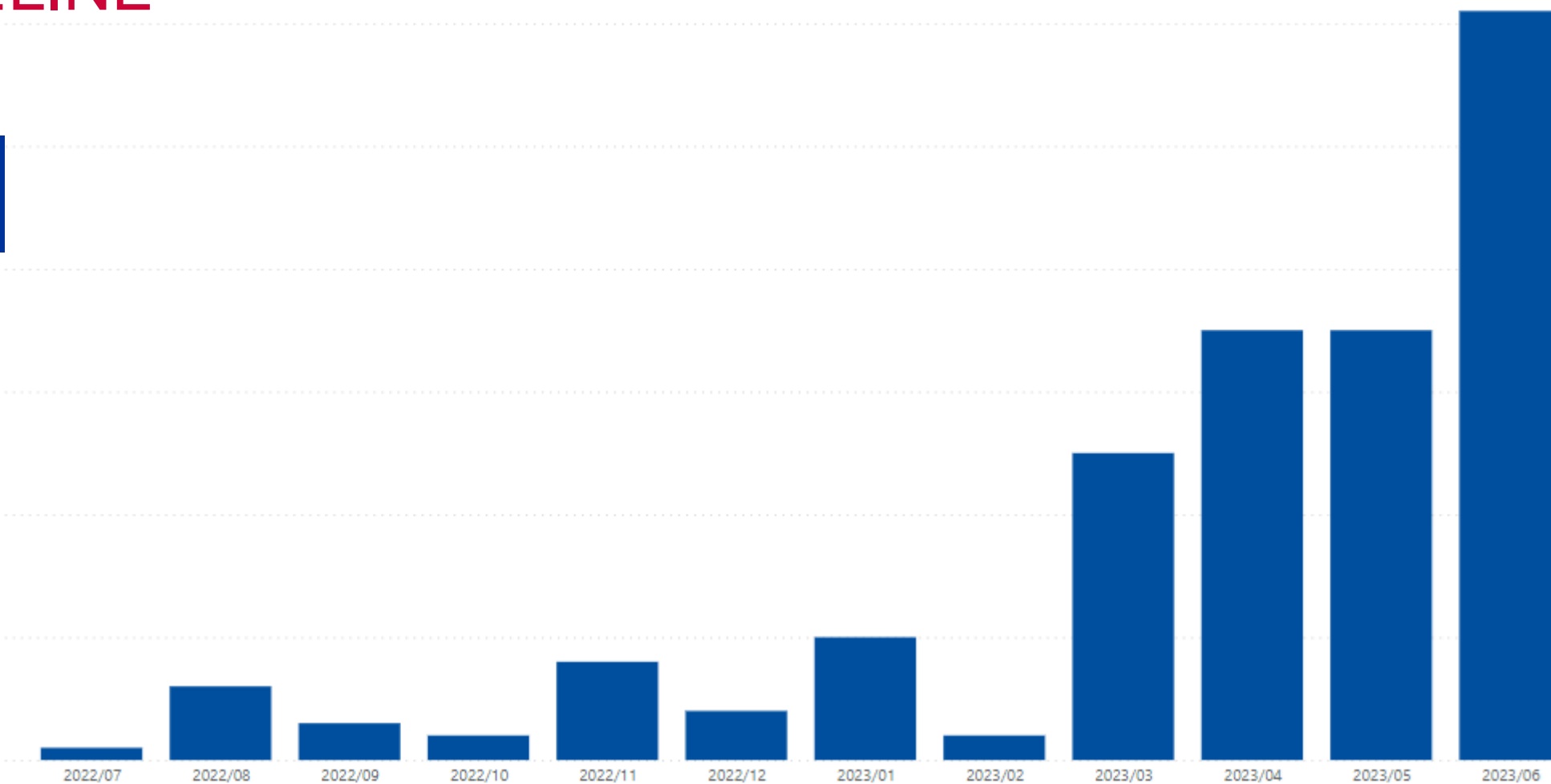
## Overall



## Transport

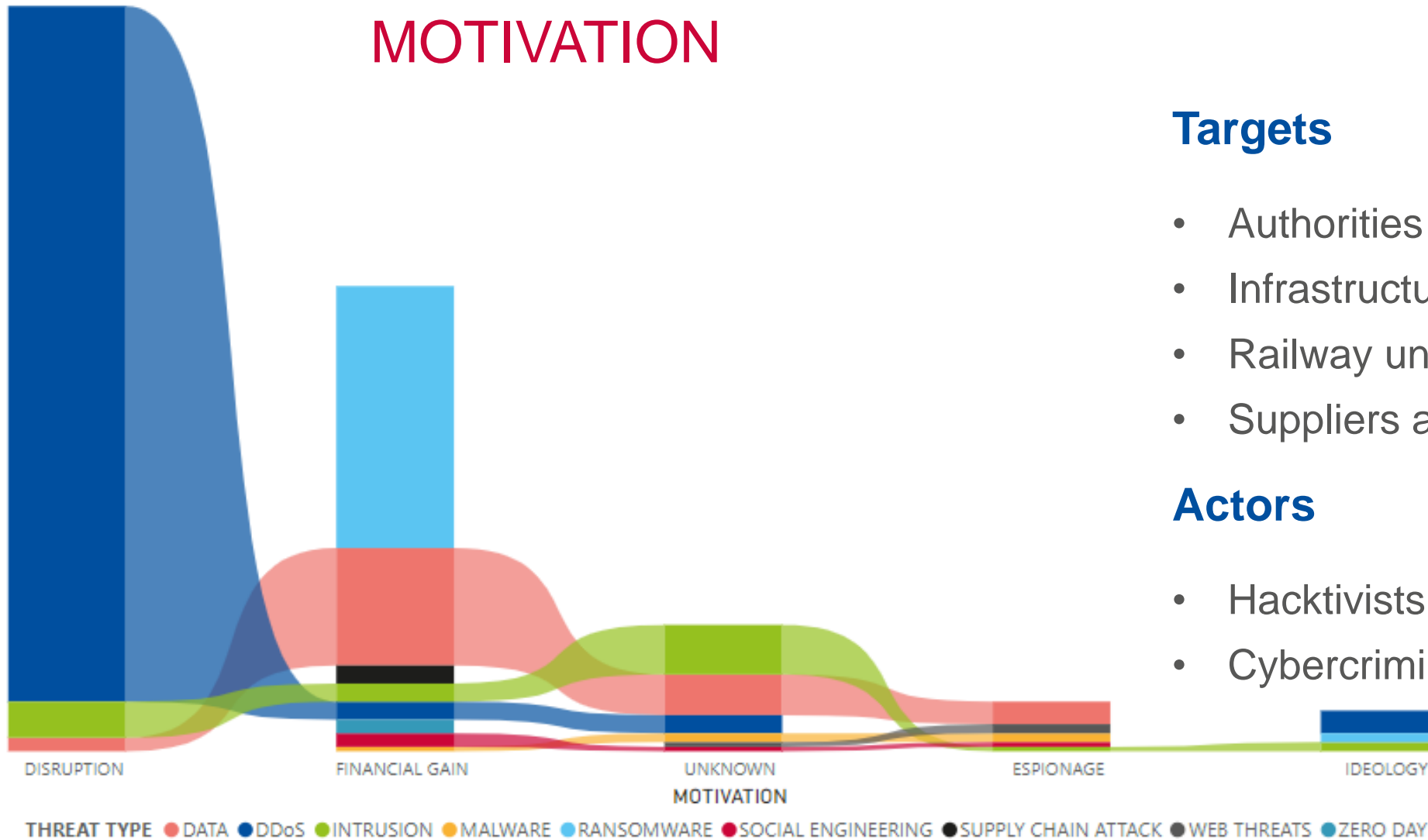


# TIMELINE



Number of incidents (Q3 2022 to Q2 2023, transport sector)

# MOTIVATION



Observed motivation per threat type (Q3 2022 to Q2 2023, transport sector)

## Targets

- Authorities
- Infrastructure managers
- Railway undertakings
- Suppliers and service providers

## Actors

- Hacktivists
- Cybercriminals

# DENIAL OF SERVICE

Increased hacktivist activity of groups with pro-Russian/anti-NATO sentiments

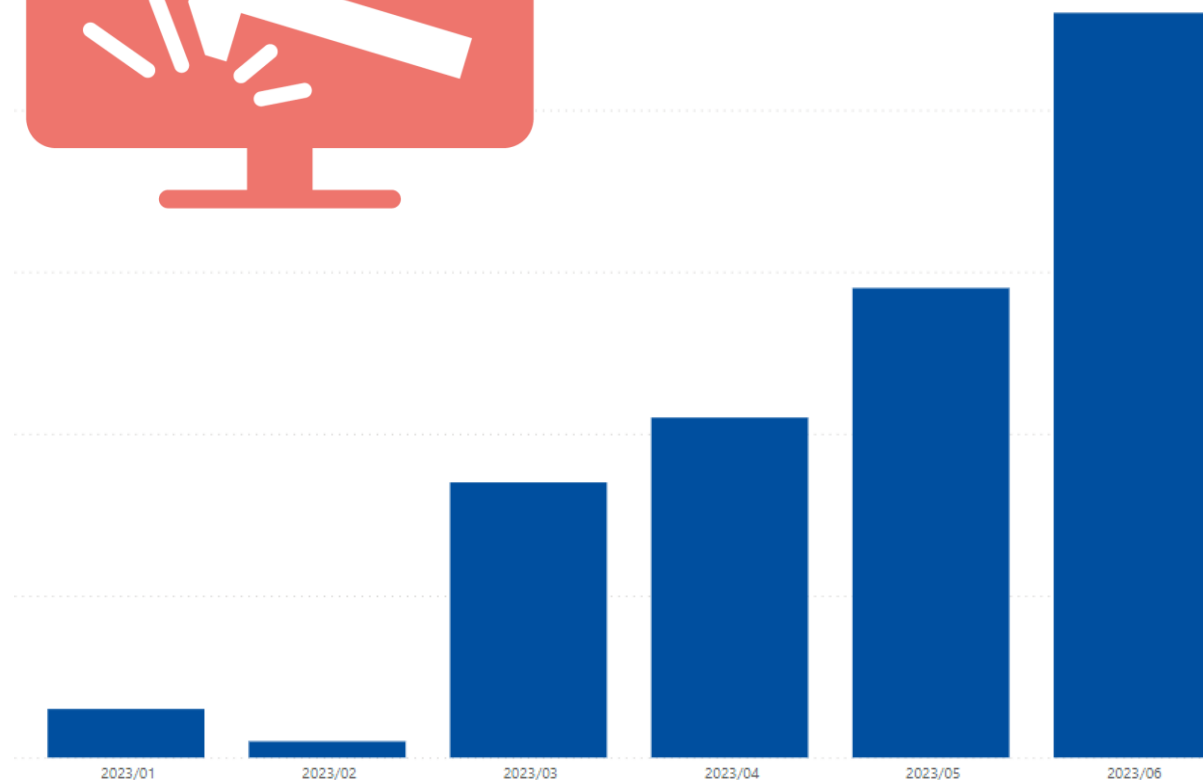
Server-class botnets, DDoS-for-Hire services and DDoS tools

IoT devices used as tools

DDoS attacks to distract from other attacks e.g. data breaches or account takeovers.

Extortion-based DDoS attack

Impact of vulnerabilities in cloud infrastructure



Rise of DoS Attacks in Q1 and Q2 of 2023 (Transport sector)

# RANSOMWARE

## Ransomware remains a significant threat

Ransomware groups: opportunistic, relatively indiscriminate in their targeting.

Ransomware attacks: not only monetary motivations – use for hacktivism due to effectiveness, impact and media attention.

Ransomware groups will likely target and disrupt OT operations.



## 2023 updates

Use of zero day vulnerabilities.

March 2023 broke ransomware attack records.

URL delivered ransomware instead of e-mail.

Fewer victims paid in 2022 but not the case for 2023 - shifting from encryption to data extortion.



# DATA RELATED THREATS

## Trends in transport

Notable data thefts.

Customer, personnel and medical records are usually stolen.

Customer data are of most value.

First publicly known case of a double-extortion ransomware attack against a US freight rail operator.



## 2023 updates

- Increase in 2023
- Lack of transparency in data breach notices
- A shift towards storing sensitive data in the cloud has been reported, with a majority of organizations indicating they now store between 21% and 60% of their data in cloud services.
- Cloud misconfigurations have been identified as a primary factor
- Instances of data breaches involving AI chatbots have been reported, compromising user payment information.

# SUPPLY CHAIN ATTACKS

## 2023 updates

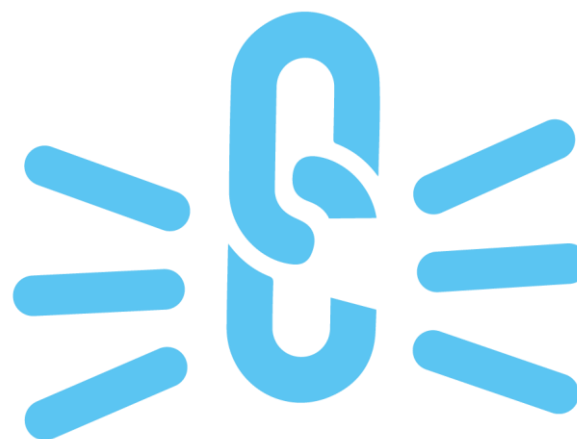
Rise in Russian cyber attacks on Ukrainian supply chains. Prestige ransomware used on transportation.

Targeting Identity Providers, MSPs and IT Suppliers

Use of Employees as Entry Points via continued targeting of employees with access privileges, personal device attacks, and social engineering, such as MFA fatigue attacks, call back phishing or QR phishing.

## Notable case

Service disruptions to an EU train operator (October 2022) due to an attack on one of its ICT service providers after an alleged DDoS attack. The incident reportedly affected the accessibility of a key safety-critical IT system, thereby disrupting operations for several hours that day.



# IS OPERATIONAL TECHNOLOGY (OT) SECURE?

- **IT systems are mainly targeted.** No reliable information on a cyber-attack affecting safety in the EU.
- **Disruptions due to the unavailability of IT services:** passenger services, ticketing systems, mobile application, display boards, etc.
- **OT systems and networks were affected:** when entire networks were disrupted or when safety-critical IT systems were unavailable.
- BUT:
- **Malware aiming at industrial disruption** (Industroyer2, INCONTROLLER, COSMICENERGY).
- **Ongoing digital transformation** and convergence between IT and OT networks
- **Urgency to pay ransom** to avoid any critical business and social impact.
- **Geopolitical tensions**, as ransomware groups are taking sides and are likely to conduct retaliatory attacks against critical western infrastructure.
- Increase in the **number of newly identified vulnerabilities in OT environments.**

# SUMMARY



**Threat actors use whatever is more relevant and evolve and adapt to the change of technologies.**

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

**Cyber attacks has increased 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

 ENISA Threat Landscape  
2023: Transport Sector

 [etl@enisa.europa.eu](mailto:etl@enisa.europa.eu)

 [www.enisa.europa.eu](http://www.enisa.europa.eu)

