enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA'S THREAT LANDSCAPE 2024

Marianthi Theocharidou,
Cyber Security Expert

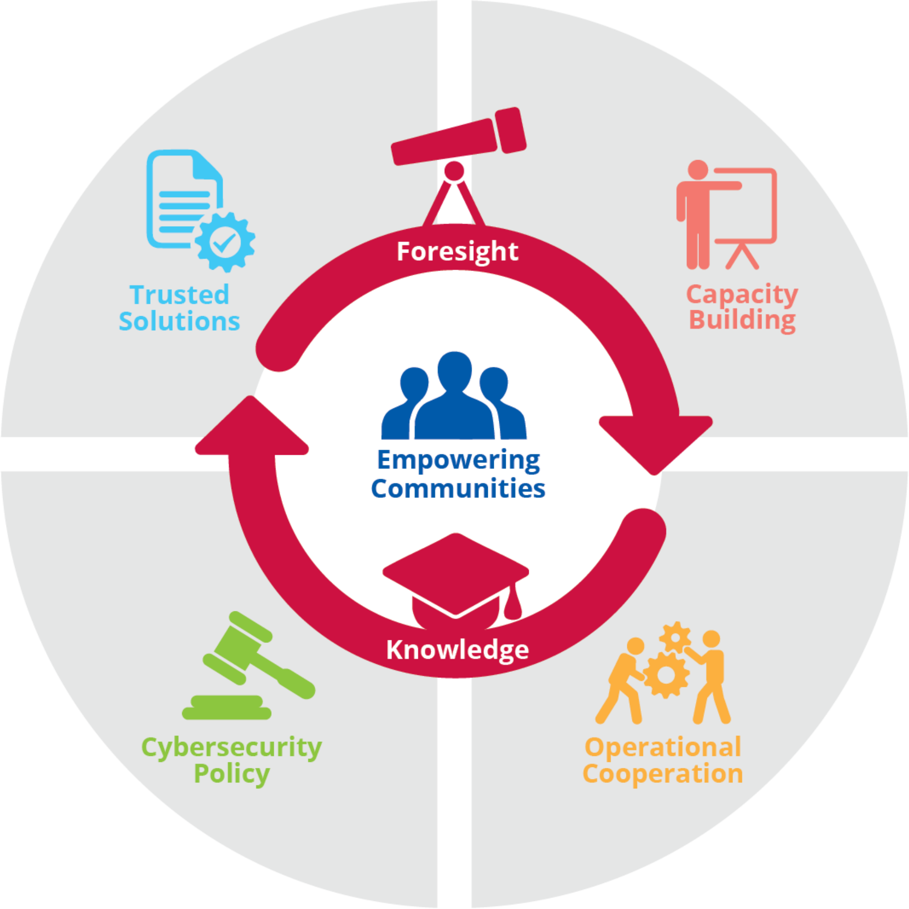
03 12 2024

ROLE OF ENISA – WHO WE ARE

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



AGENDA

- ENISA Threat Landscape activity & methodology
- Threat actors
- Prime threats

ENISA THREAT LANDSCAPE TRADITION

enisa 20 years!

EUROPEAN UNION AGENCY FOR CYBERSECURITY

ENISA THREAT LANDSCAPE 2024

July 2023 to June 2024

SEPTEMBER 2024

EUROPEAN UNION AGENCY FOR CYBERSECURITY

AT
2023

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

022

EUROPEAN UNION AGENCY FOR CYBERSECURITY

EAT
E 2021

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

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

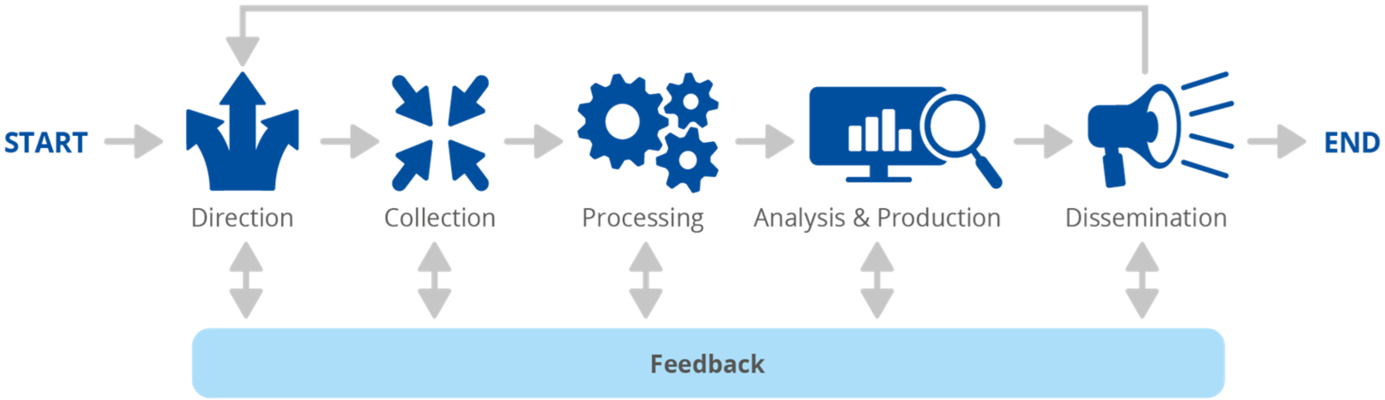
ENISA THREAT LANDSCAPE: TRANSPORT SECTOR

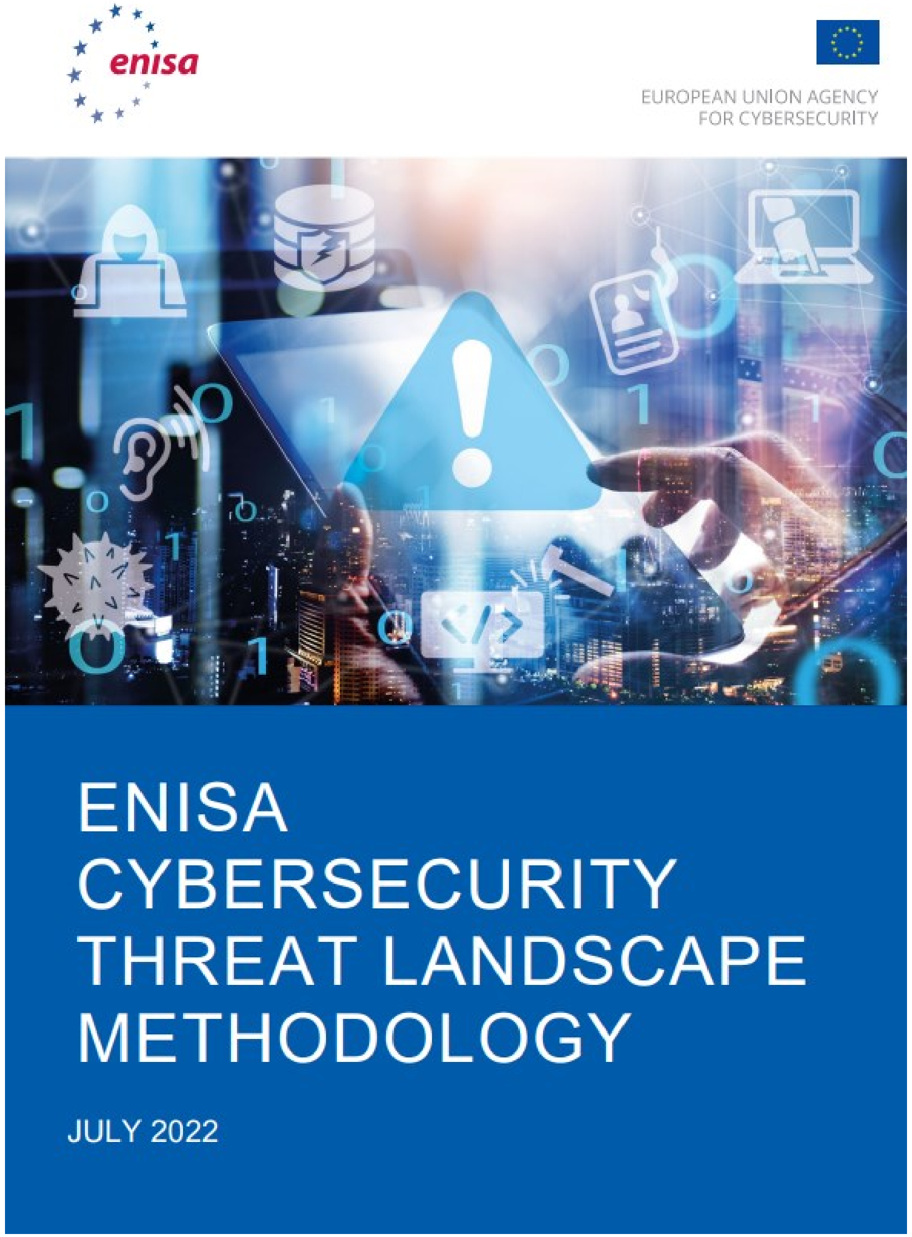
(January 2021 to October 2022)

MARCH 2023

THREAT LANDSCAPE METHODOLOGY

The ENISA Cybersecurity Threat Landscape (CTL) Methodology describes a systematic process for relevant data collection and analysis, to be used for the formation of CTLs



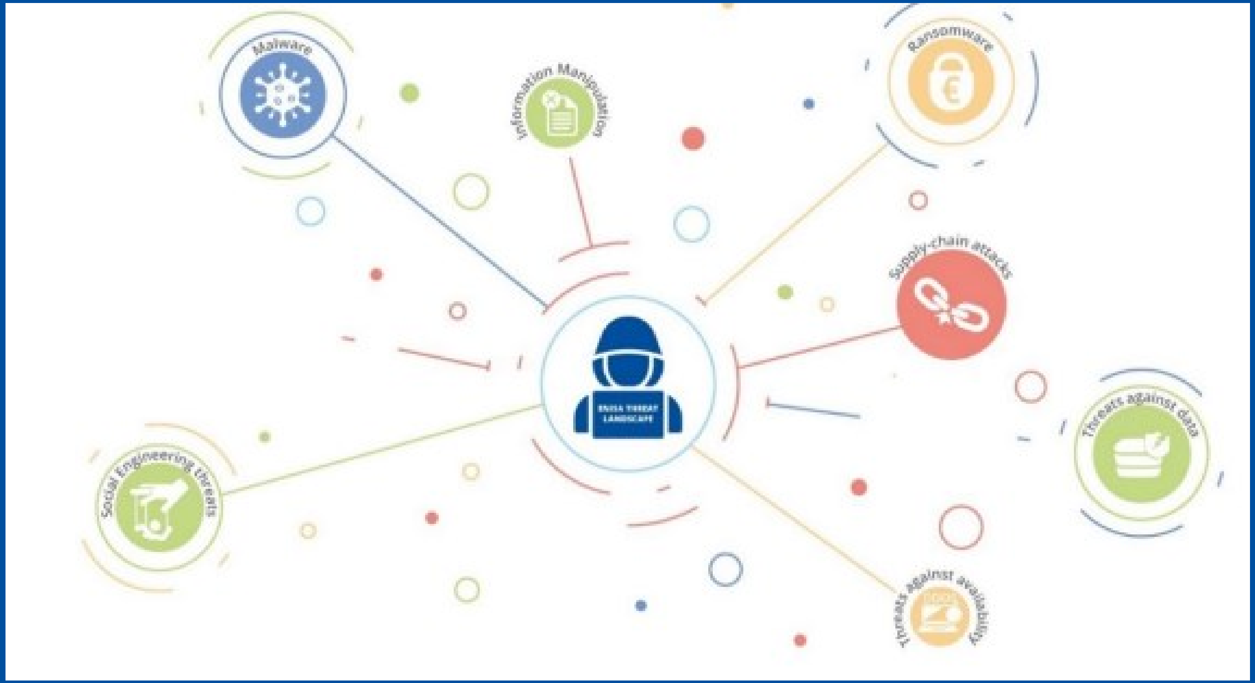

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

ENISA CYBERSECURITY THREAT LANDSCAPE METHODOLOGY

JULY 2022

ENISA
THREAT
LANDSCAPE
2024

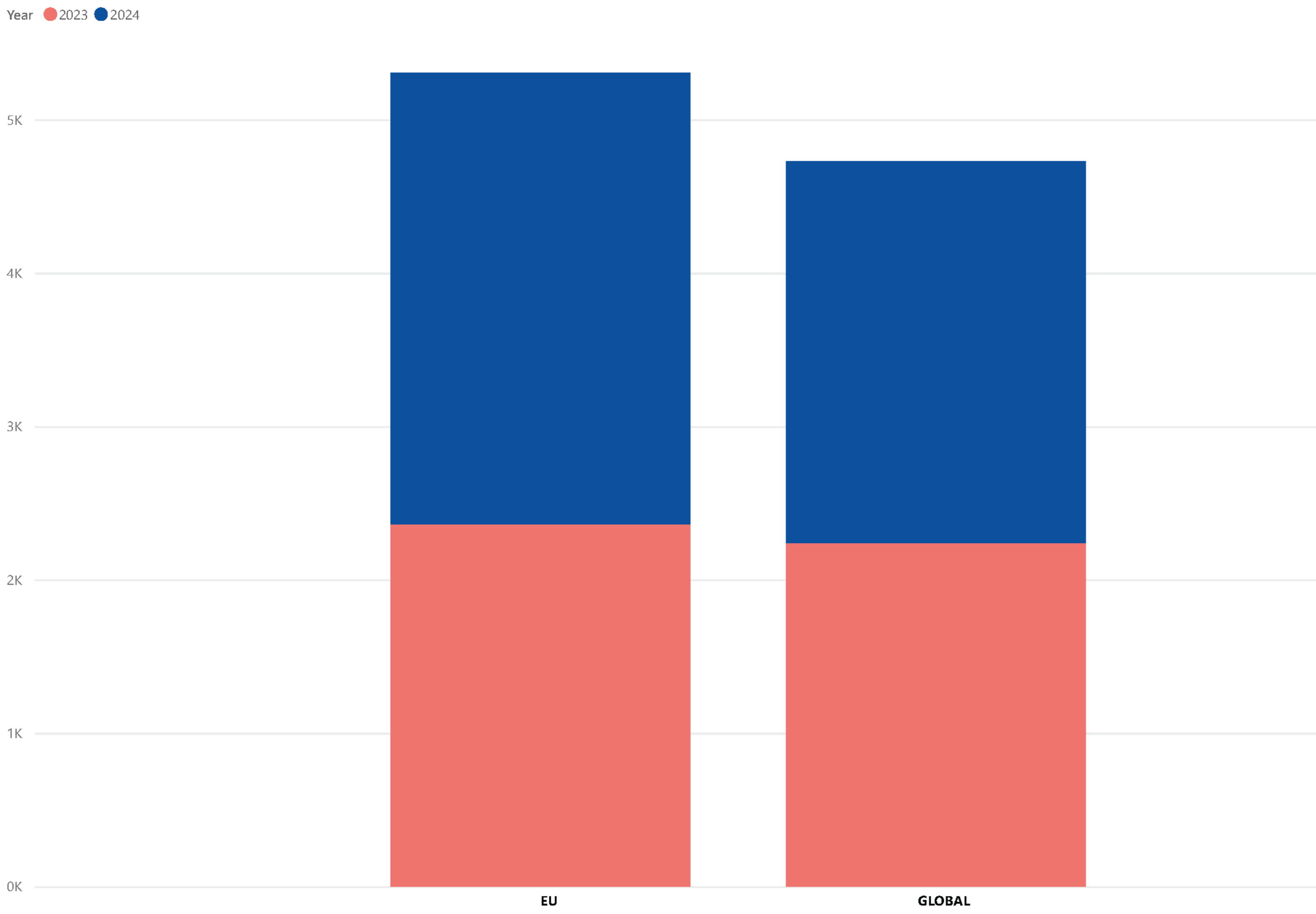


INCIDENTS
JULY 2023 TO JUNE 2024

Total

2023 – Global 2239, EU 2360

2024 – Global 2491, EU 2945



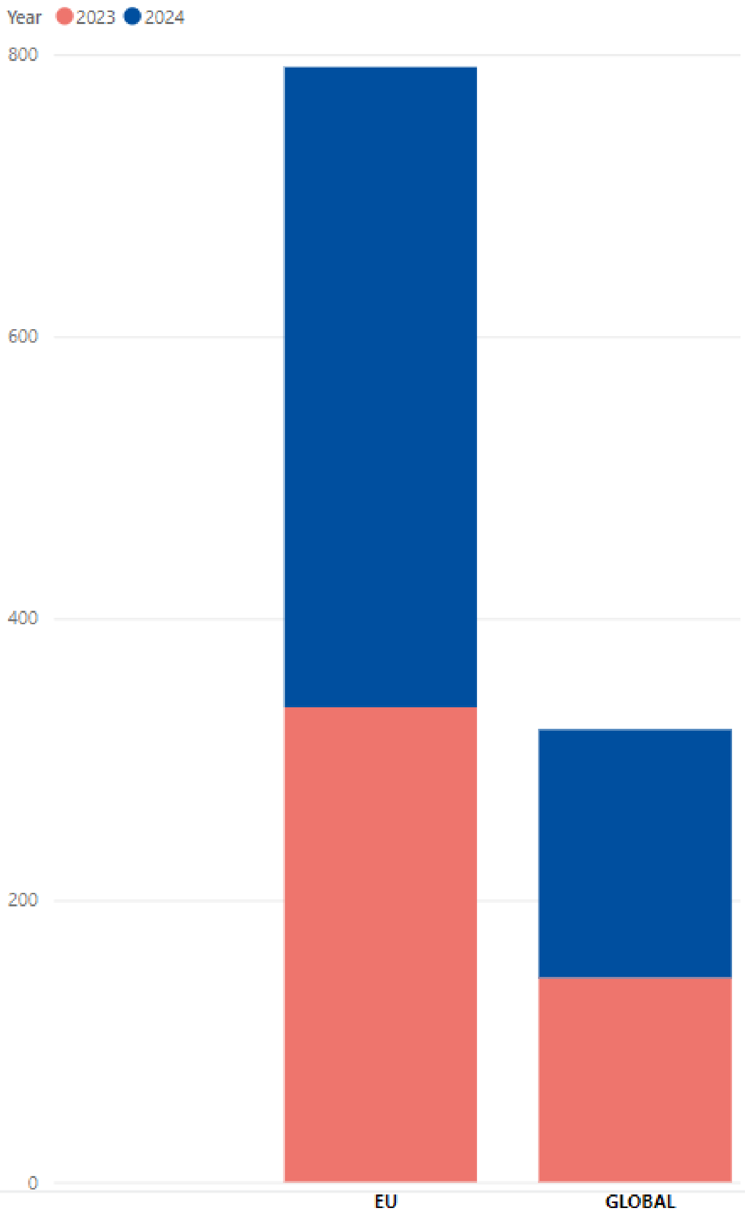
INCIDENTS (TRANSPORT)

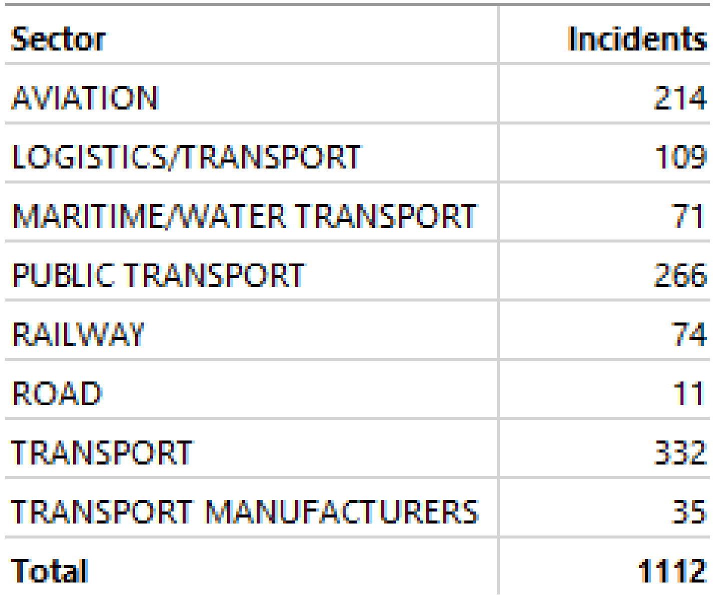
Total (July 2023 to June 2024)

2023 – Global 145, EU 337

2024 – Global 176, EU 454

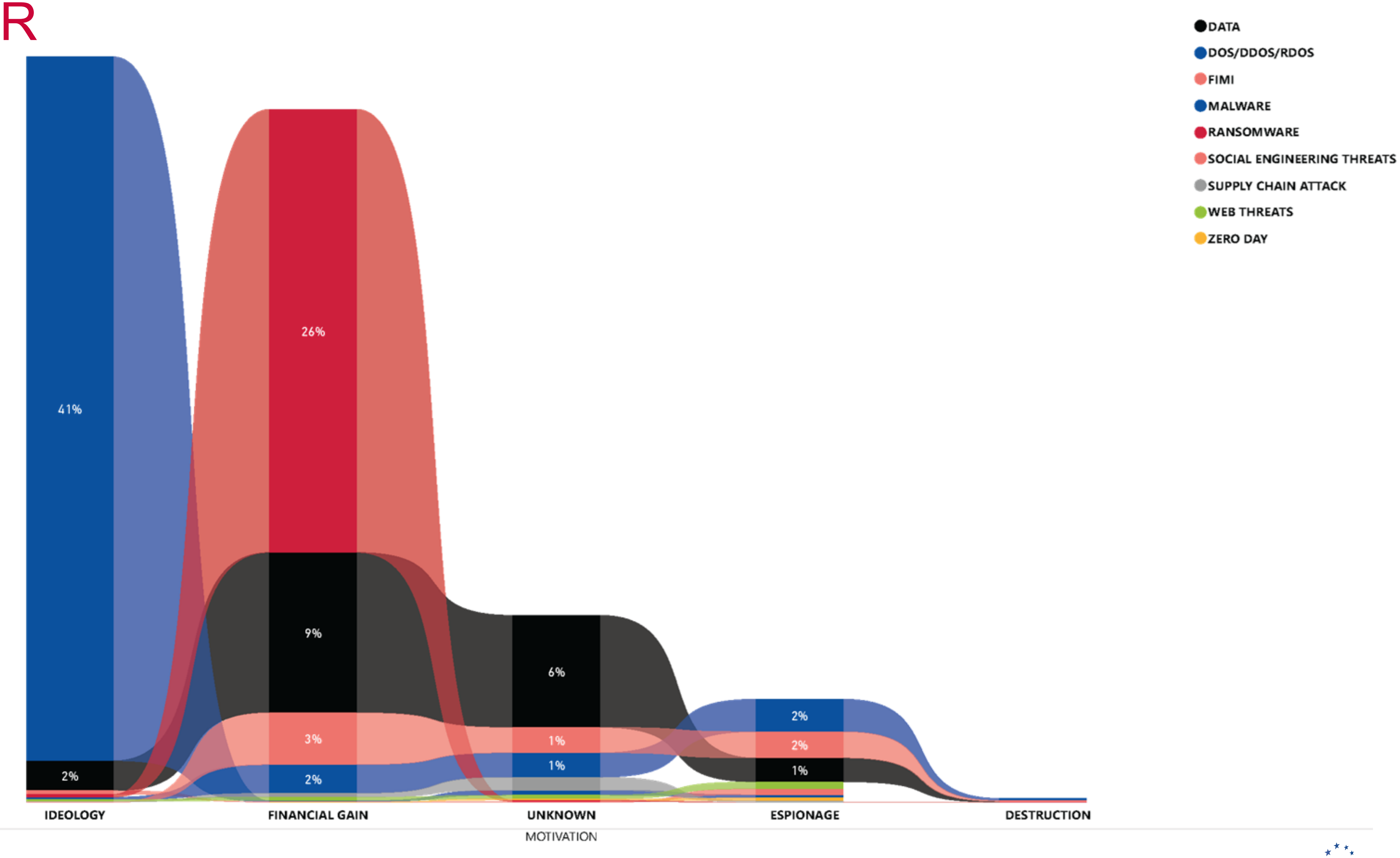
11% of total incidents
2nd most targeted sector



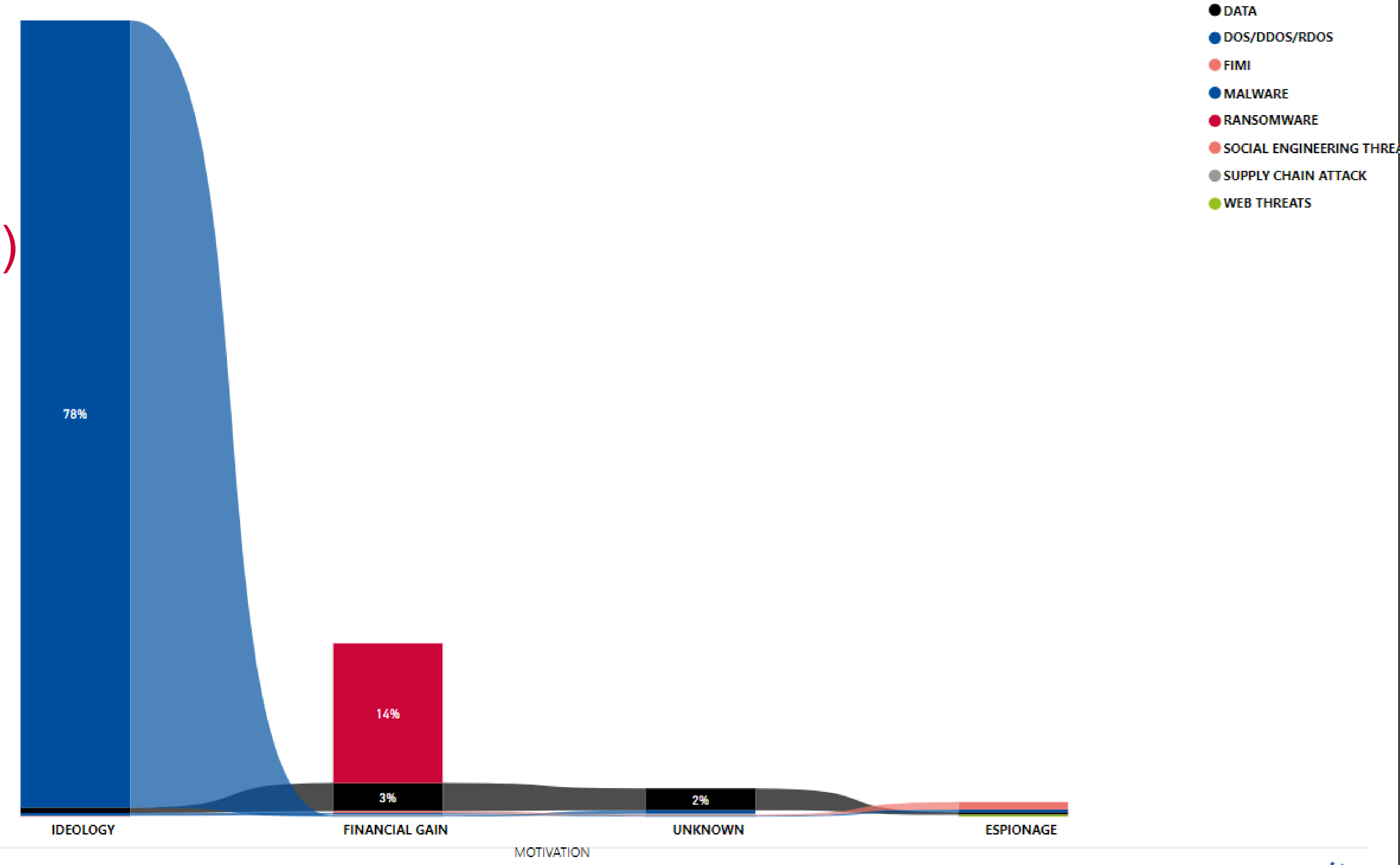


Sector	Incidents
AVIATION	214
LOGISTICS/TRANSPORT	109
MARITIME/WATER TRANSPORT	71
PUBLIC TRANSPORT	266
RAILWAY	74
ROAD	11
TRANSPORT	332
TRANSPORT MANUFACTURERS	35
Total	**1112**

THREAT ACTOR MOTIVATION



THREAT ACTOR MOTIVATION (TRANSPORT)



THREAT ACTORS

State-Nexus Actors:

Increased focus on stealth and long-term espionage operations.

Exploitation of cloud services and public-facing vulnerabilities for covert access.

Cybercrime Actors:

Growth of as-a-service ecosystems, including Ransomware-as-a-Service (RaaS) and Drainer-as-a-Service.

Increased use of AI tools for phishing, scripting, and evasion.

Hacktivists:

Alignment with geopolitical conflicts (e.g., Ukraine, Middle East).

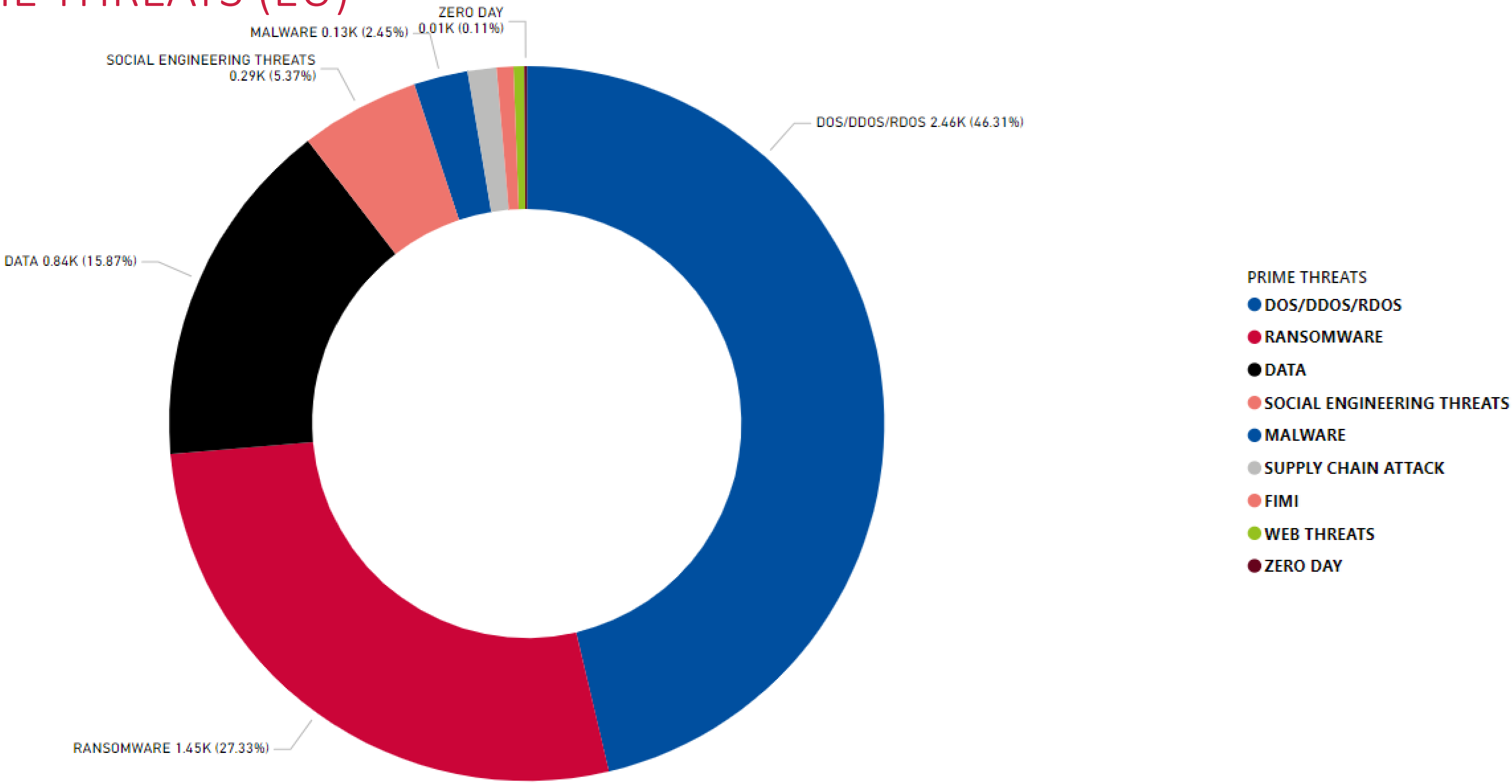
Greater overlap with state-backed operations to obscure direct involvement.

Private Sector Offensive Actors (PSOAs):

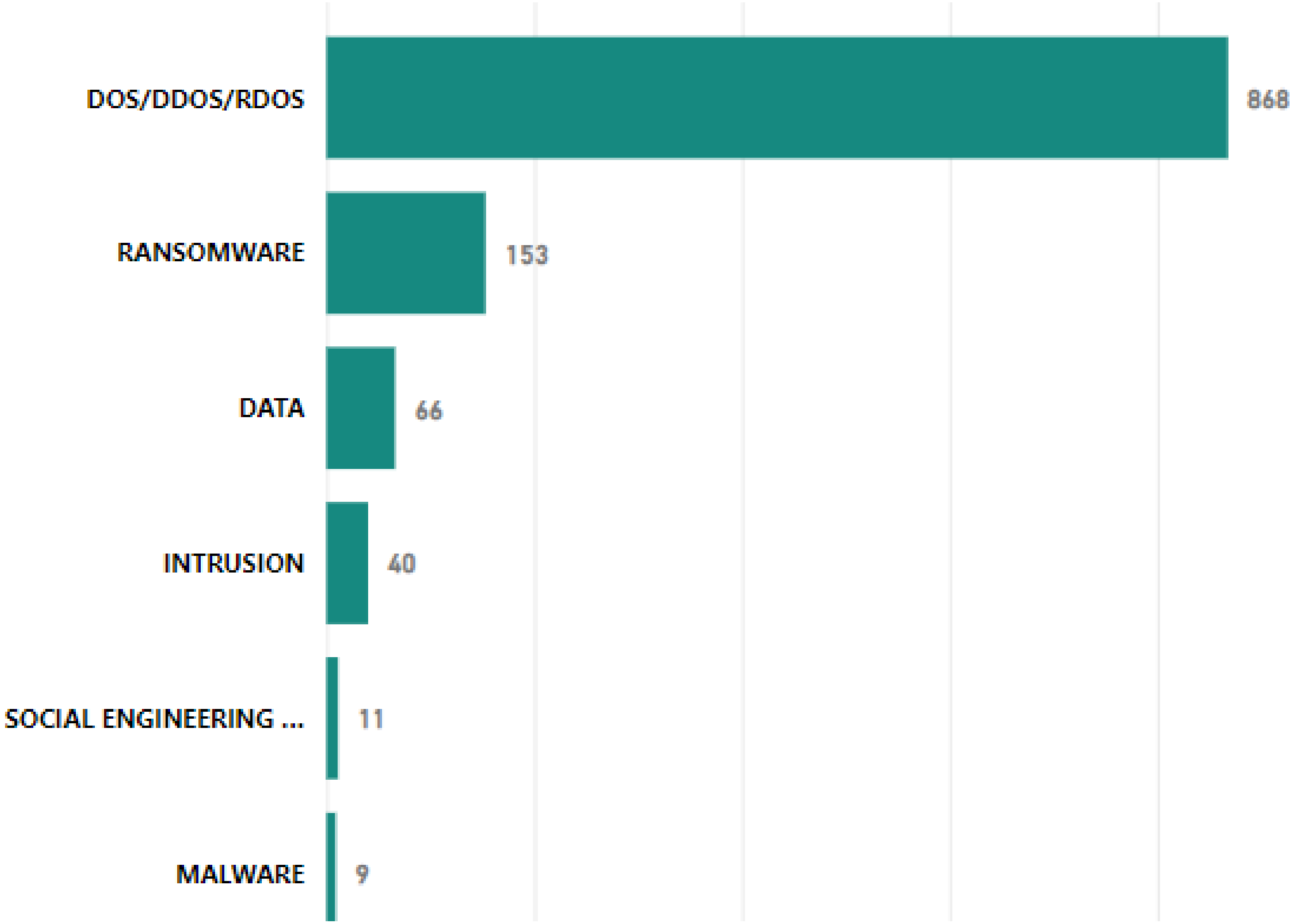
Advanced surveillance tools targeting high-value individuals and organizations.

Persistent ethical and legal concerns about their operations.

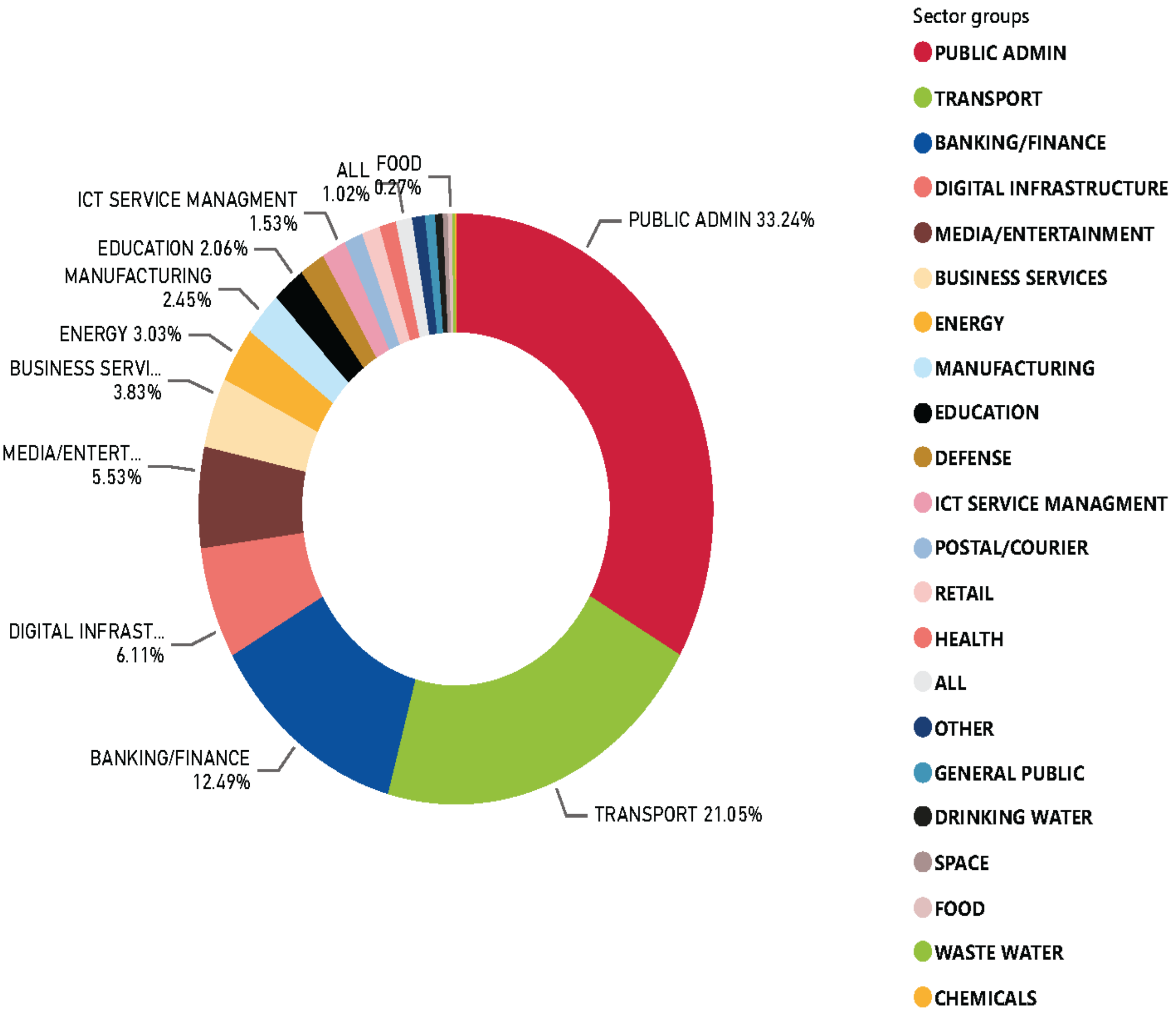
PRIME THREATS (EU)



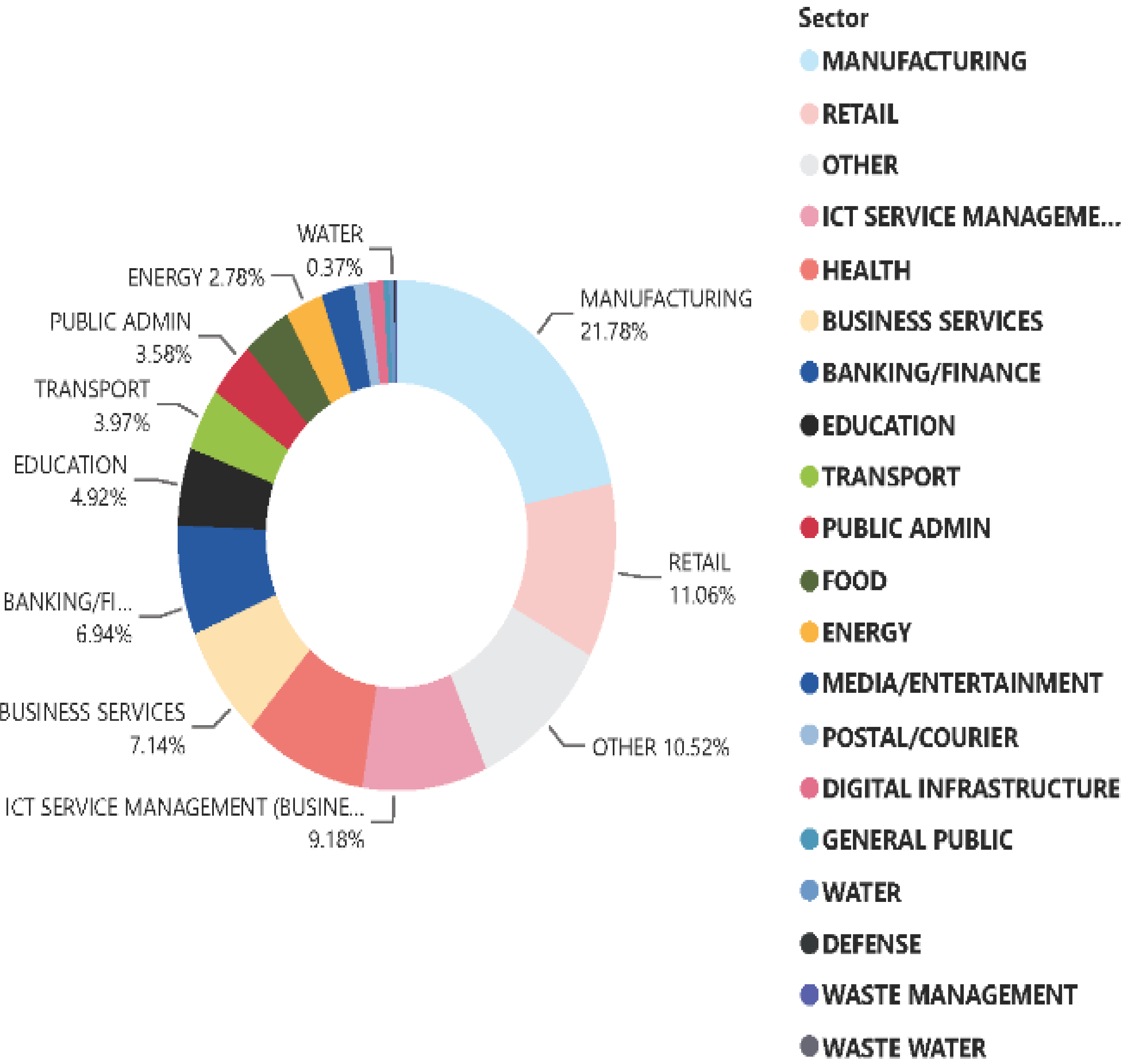
PRIME THREATS (TRANSPORT)



DENIAL OF SERVICE

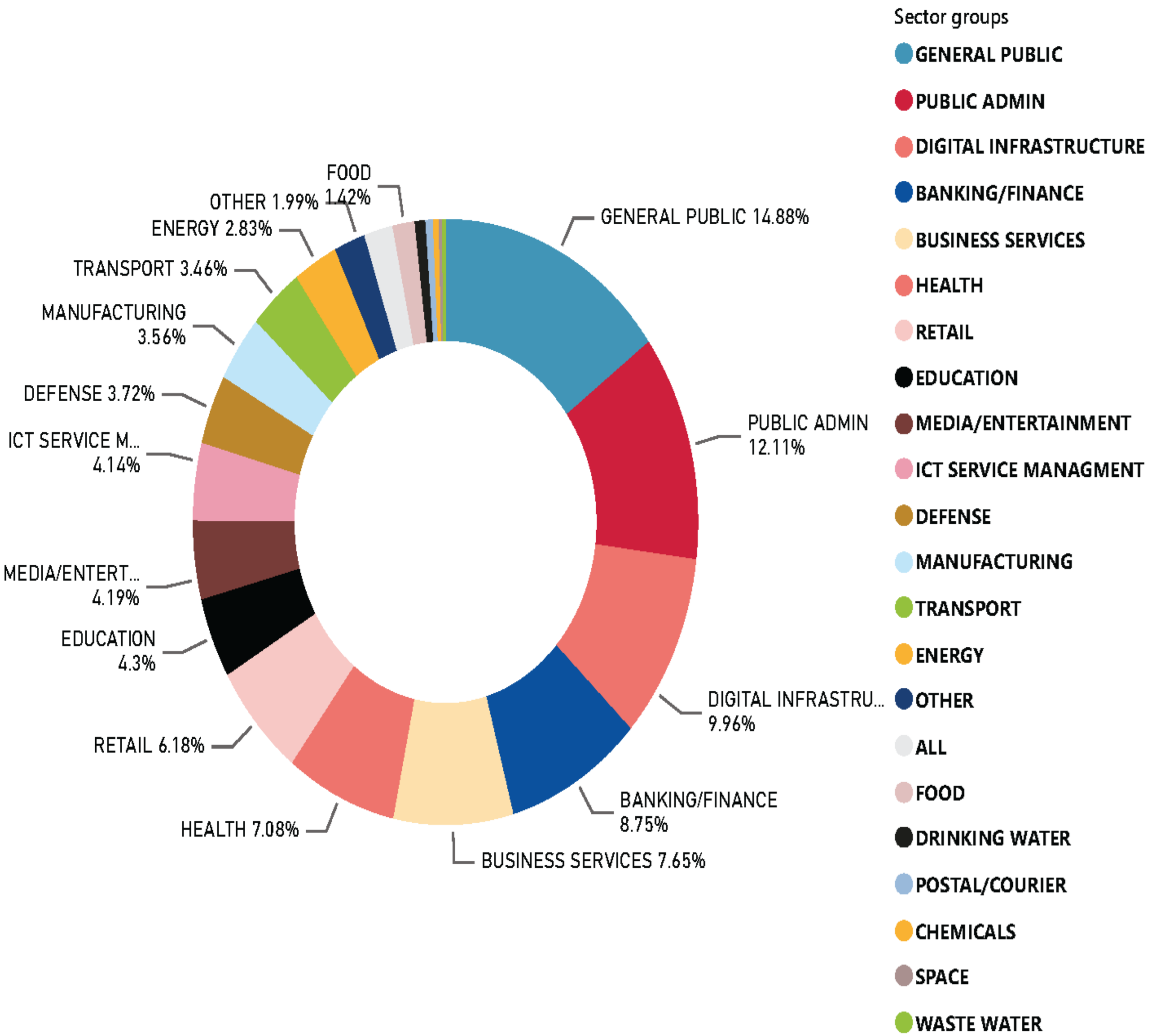


- Surge in **DDoS-for-Hire** services, enabling non-skilled attackers to launch sophisticated campaigns.
- Increased targeting of critical infrastructure sectors such as **transportation** and **energy**.
- **Higher usage of botnets** composed of compromised **residential and mobile devices**.
- EU Member States face rising DDoS incidents **driven by hacktivist and geopolitical motivations**.



RANSOMWARE

- **Stabilization of ransomware incidents** at high volumes (1,000+ claims per quarter).
- Some groups **skip encryption** and move directly to **data theft for extortion.**
- **Increased activity from strains like LockBit, Cl0p, and PLAY,** with LockBit dominating in both EU and global contexts.
- Exploitation of **supply chain vulnerabilities.**
- **Industrial and manufacturing sectors** are the most frequently targeted.
- **Retailers and digital service providers** targeted due to sensitive customer data.
- Use of **zero-day vulnerabilities** for lateral movement in virtualized environments.
- **Weaponization of regulatory requirements** (e.g., GDPR breach disclosure timelines).



DATA THREATS

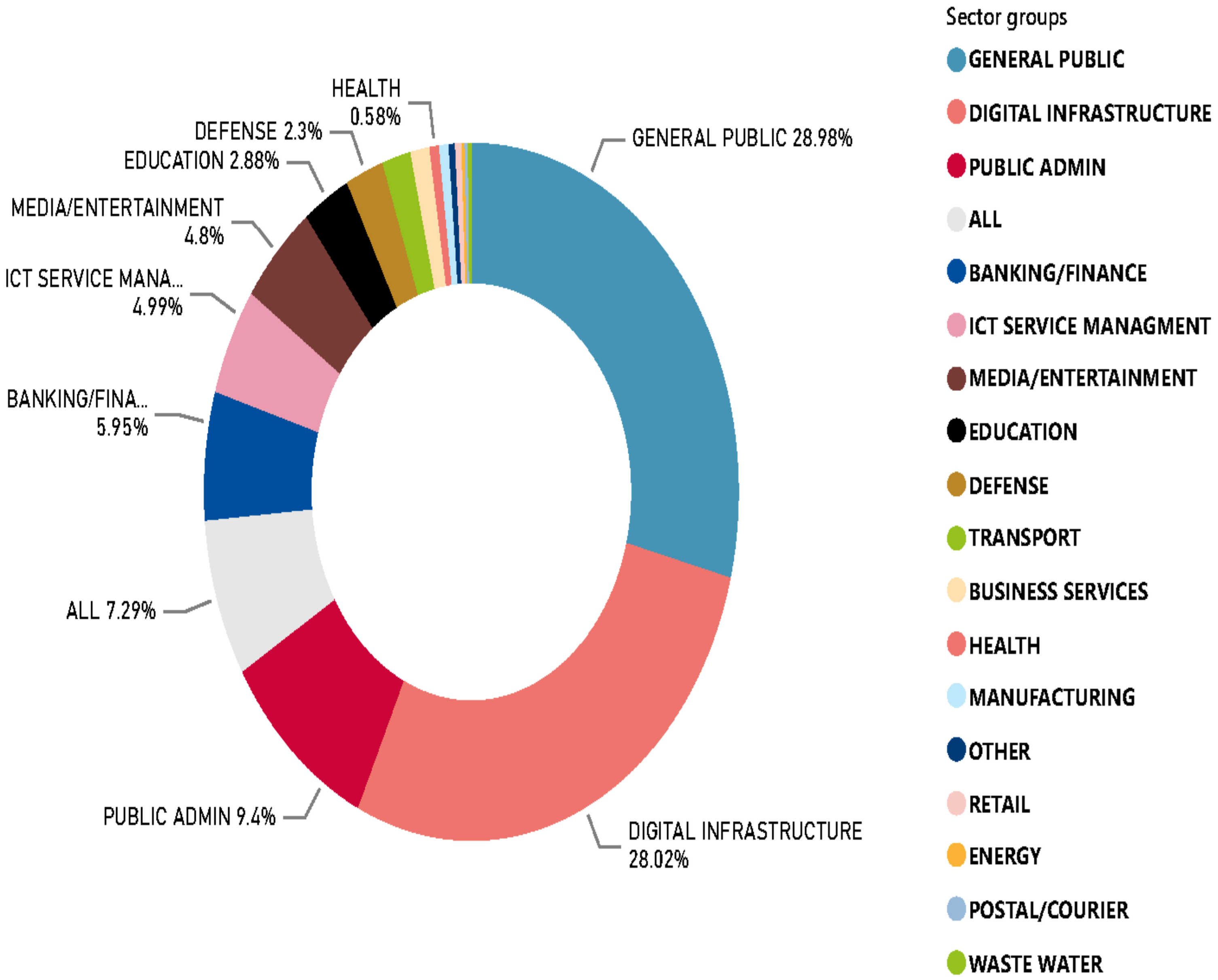
•Data breaches increasingly **paired with ransomware attacks** to amplify pressure on victims.

•Rise in **targeted attacks on GDPR compliance**, leveraging regulatory requirements for extortion.

•**Exploitation of vulnerabilities** in **cloud** storage and management platforms for data theft.

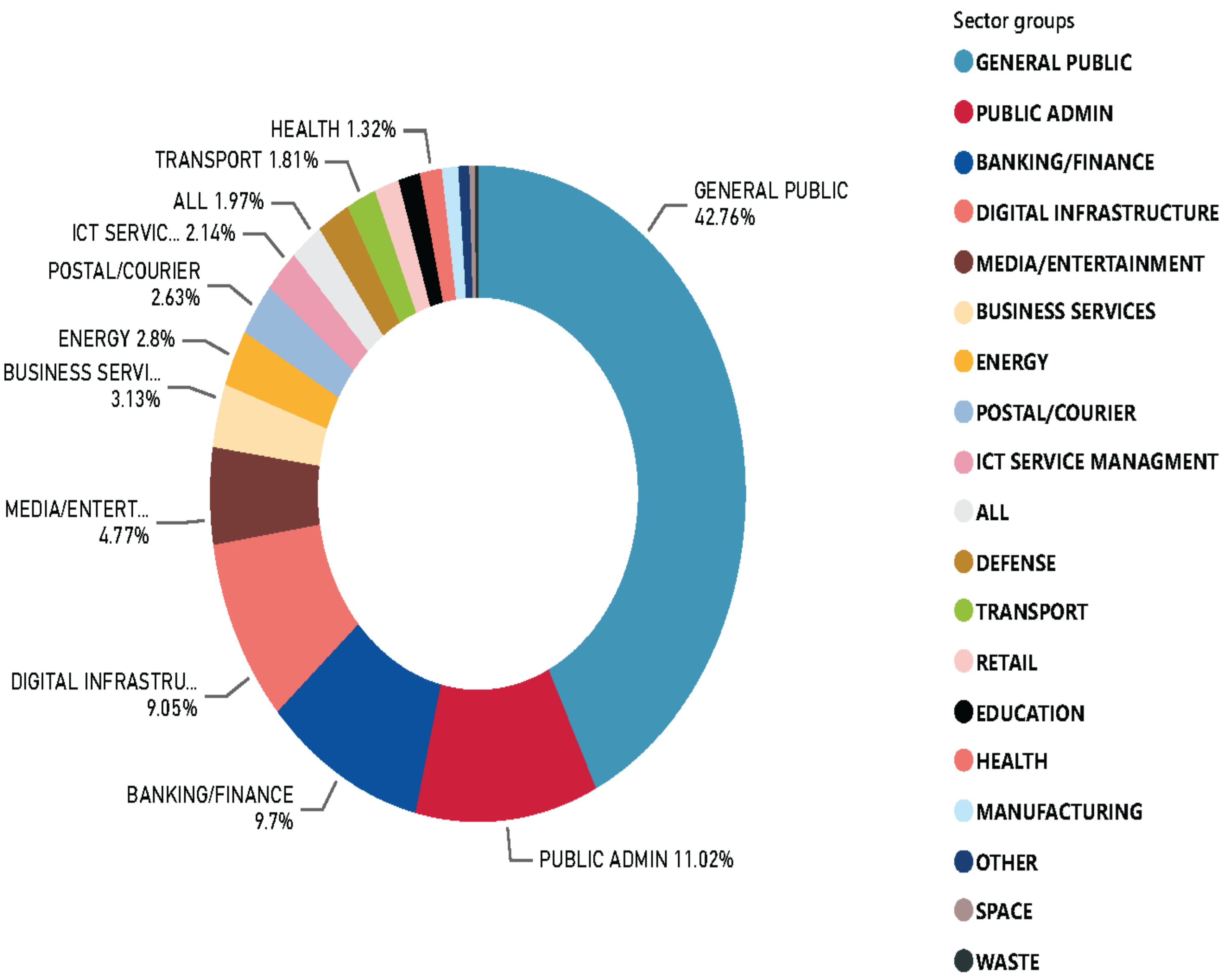
•**Public administration, finance, and digital infrastructure** sectors face the highest volume of attacks.

MALWARE



- Stealing **credentials**, deploying **loaders for other malware**, or **exploiting vulnerabilities** to establish footholds.
- Surge in **Malware-as-a-Service (MaaS)** platforms like BunnyLoader and Stealc.
- **Information stealers** (e.g., RedLine, Raccoon), often deployed via phishing and malvertising.
- **Platform Expansion:** macOS systems increasingly targeted.
- **Innovations in Malware:**
- Use of advanced loaders to bypass traditional detection mechanisms.
- Deployment via trusted platforms such as GitHub, Google Drive, and Slack.

SOCIAL ENGINEERING THREATS



- **Phishing, spear-phishing, QR phishing, smishing, and vishing**.
- Use of **scare tactics** or **impersonation** to gain access to sensitive information.
- Sharp increase in **Business Email Compromise (BEC)** campaigns due to low detection rates.
- **AI-powered phishing campaigns** using tools like FraudGPT to craft convincing lures.
- Rise of **deepfake-based scams**, particularly targeting executives and high-value individuals.
- Growth of **Adversary-in-the-Middle (AitM) phishing tools** like Evilginx, bypassing MFA protections.
- **SEO poisoning** targeting users searching for legitimate resources or software.

SUMMARY-THREATS

Ransomware stabilized at high volumes with increased focus on double and triple extortion techniques.

•Surge in Malware-as-a-Service offerings and targeting of macOS platforms.

•Popularity of information stealers in attack chains.

•AI-driven phishing and deepfake campaigns growing in sophistication.

•Business Email Compromise (BEC) as a persistent threat.

•Expansion of DDoS-for-Hire services targeting critical infrastructure.

•AI-enhanced disinformation campaigns tailored to regional contexts.

THANK YOU FOR YOUR ATTENTION

Agamemnonos 14, Chalandri 15231
Attiki, Greece

info@enisa.europa.eu

www.enisa.europa.eu