

ENISA THREAT LANDSCAPE

OCTOBER 2025



Threat Overview

Top 5 targeted sectors in the EU

These reportedly include **public administration, transport, digital infrastructure and services, finance, and manufacturing**, with essential entities representing 53.7% of the total number of recorded incidents.

State-aligned operations against EU Member States organisations persist

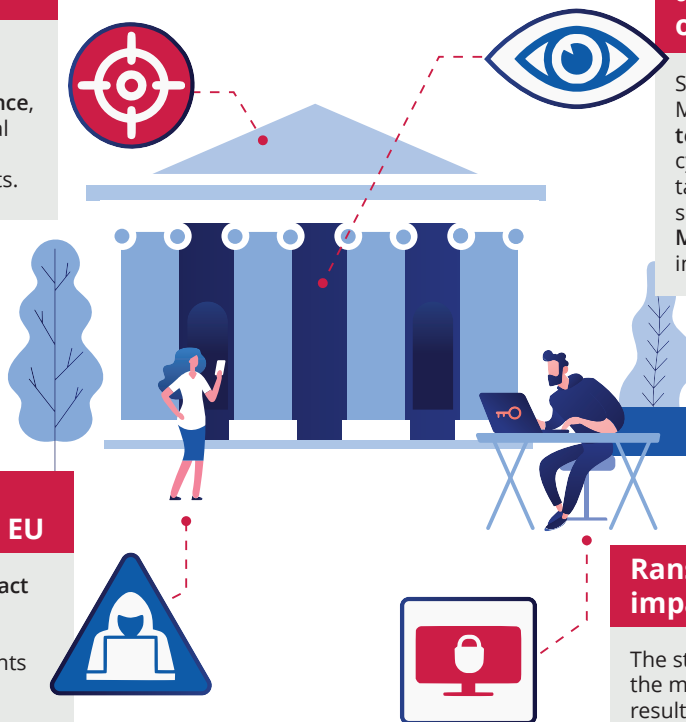
State-aligned activities against EU Member States **continued at a steady tempo**, with state-nexus cyberespionage activities notably targeting the public administration sector, and **Foreign Information Manipulation and Interference (FIMI)** increasingly targeting EU audiences.

Hacktivism dominates incident volume in the EU

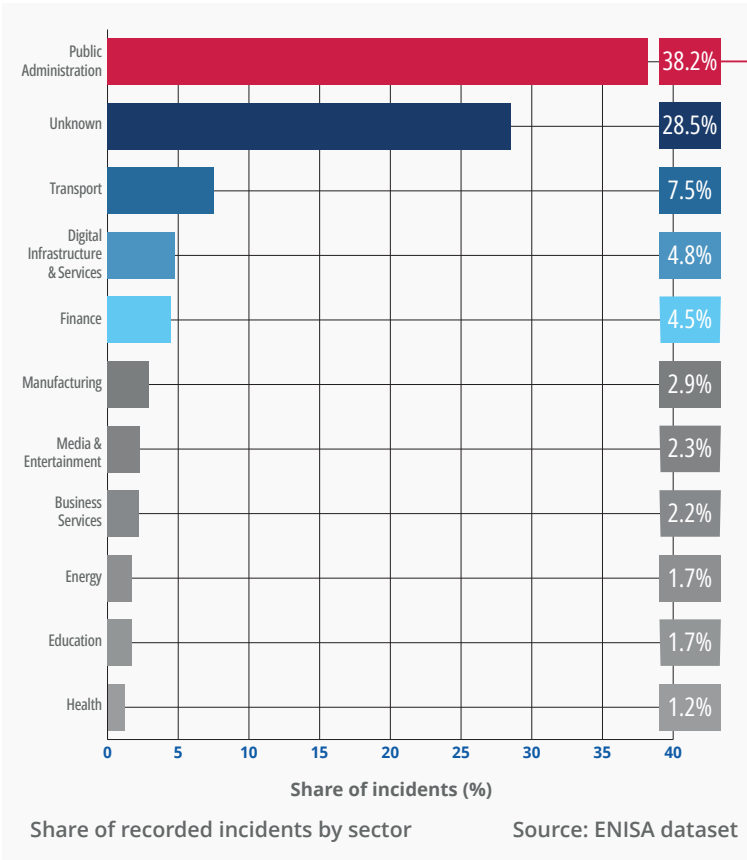
It was mainly driven by **low-impact DDoS campaigns** targeting EU Member States' organisations' websites, with only 2% of incidents leading to service disruption.

Ransomware remains the most impactful threat in the EU

The strains **Akira** and **SafePay** were among the most deployed, with a few incidents resulting in service disruptions.





Sectorial overview




38.2% Public Administration

Public Administration was identified as the most targeted sector in the EU (38.5%), dominated by low-impact DDoS (94.8%), with ransomware particularly affecting municipalities.



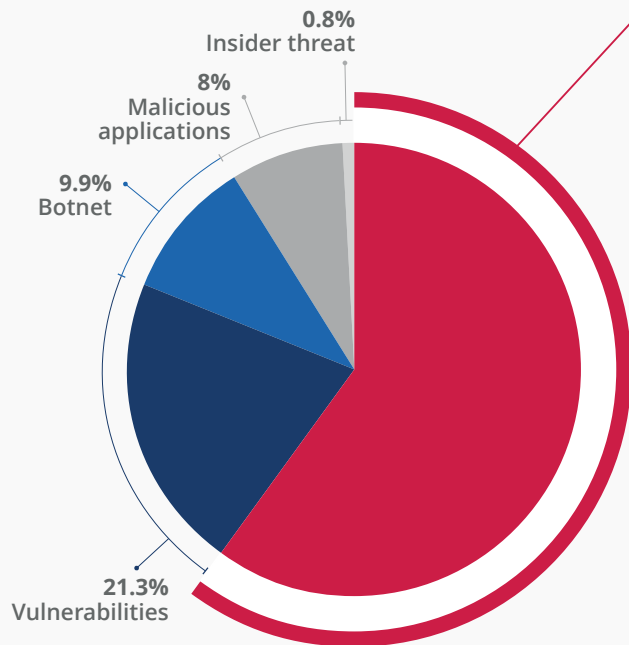


The **transport sector** came in second (7.5%), with most reported incidents pertaining to air and logistics, with a particular focus on targeting the maritime sector displayed by state-nexus intrusion sets.



While reportedly less targeted (2.2%), **digital infra- structure and services in the EU**, including Digital Services Providers remain high-value targets, particularly in the frame of incidents leveraging cyber dependencies used as launchpads for follow-up attacks.

Tactics, Techniques and Procedures overview



Most identified initial infection vector

Source: ENISA dataset

60% Phishing

Phishing was the dominant intrusion vector, accounting for approx. 60% of cases, including malspam, vishing, and malvertising. Vulnerability exploitation represented 21.3% of initial access vectors, with 68% leading to malware deployment as a follow-up activity.

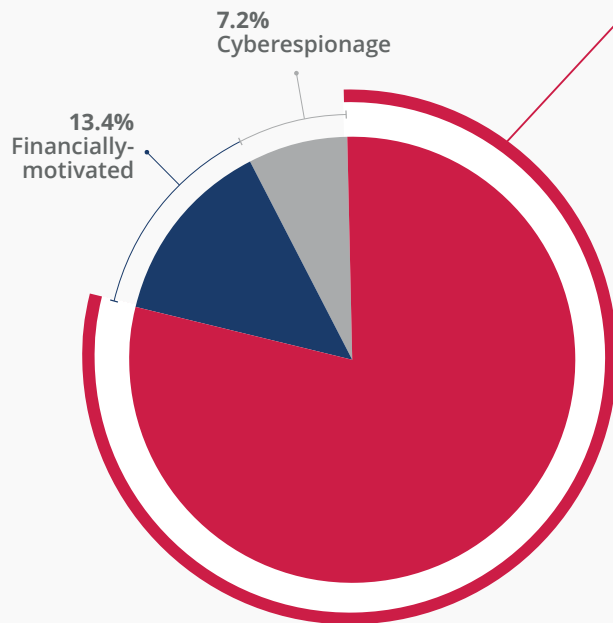


Mobile devices and Internet-exposed services and devices, particularly Operational Technology (OT) systems remain high value targets across all types of threats.



State-aligned intrusion sets and cybercriminal operators increasingly leverage AI for productivity and optimisation of their malicious activities.

Threat-centric overview



Distribution of assessed objectives

Source: ENISA dataset

79.4% Ideology driven

NoName057(16) was responsible for over 60% of claims, sustained by its DDoSia platform, with activity spikes pertaining to EU support to geopolitical events and national elections.



Despite a reported decrease of 11% compared to the previous ETL, **ransomware** remained the most impactful cybercrime tool. Initial Access Brokers continued trading low-cost, high-volume VPN and RDP access.



Among state-nexus intrusion sets, **APT28**, **APT29**, and **Sandworm** were reportedly the most active in the EU, notably targeting public administration, defence, and telecommunications entities. **The Matryoshka Information Manipulation Set** was reported the most active in FIMI campaigns.



ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.



Catalogue number: TP-01-25-025-EN-N

ISBN: 978-92-9204-721-4

DOI: 10.2824/2445233

ENISA

European Union Agency for Cybersecurity

Athens Office

Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office

Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu



Publications Office
of the European Union