



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EU THREAT LANDSCAPE 2026

ENISA Webinar

29/09/2026

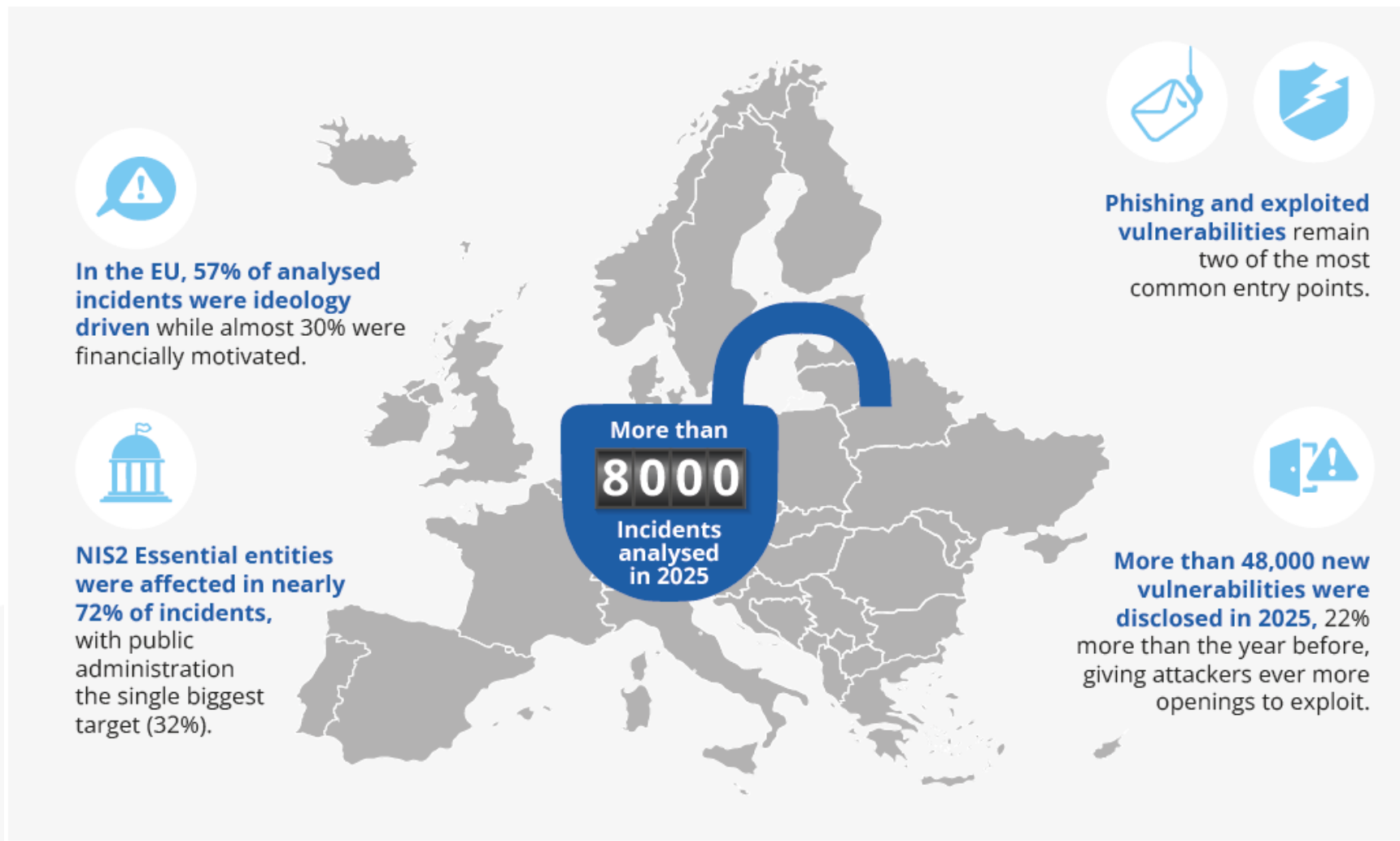
TLP:CLEAR

ETL METHODOLOGY

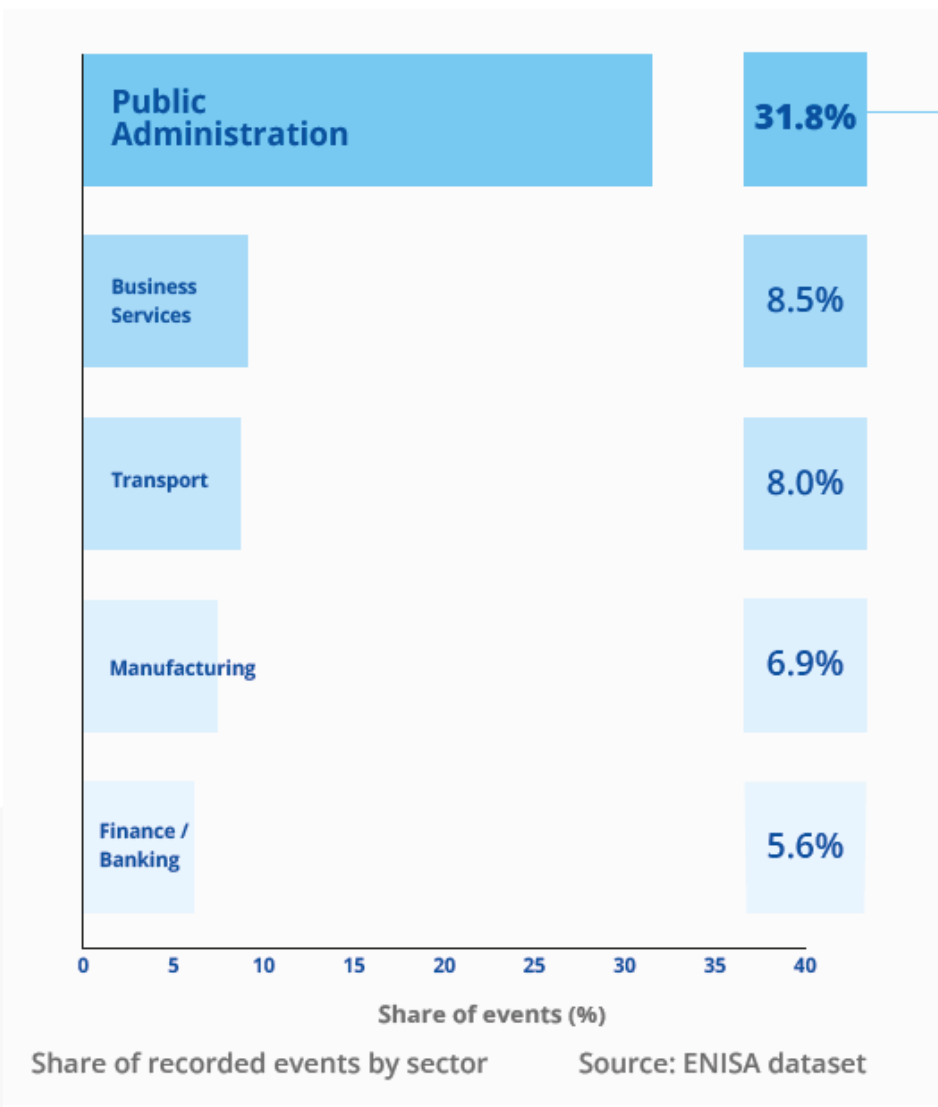


<https://www.enisa.europa.eu/publications/enisa-cybersecurity-threat-landscape-methodology>

THREAT OVERVIEW



SECTORAL OVERVIEW



Public Administration

remains the most targeted sector, accounting for almost 32% of all recorded events. The events primarily impacted central (35.1%) and local entities (33.8%).



Business services



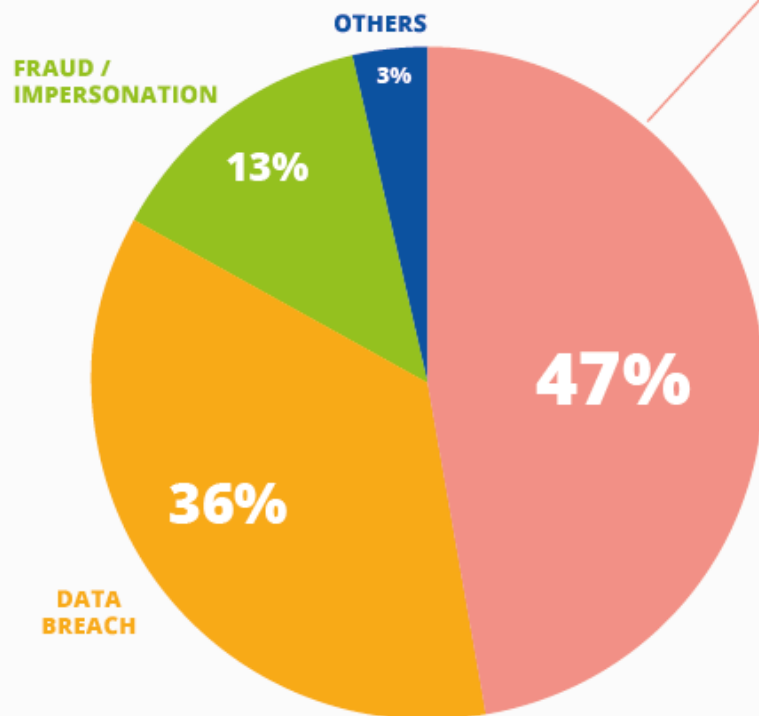
The business sector is primarily impacted by unauthorised accesses (57%), followed by DDoS attacks (38%). Recorded unauthorised accesses included ransomware and data breaches. Hospitality, consultancy and broadcast media together accounted for 55% of events impacting this sector.

Transport



The transport sector remained largely impacted by DDoS claims (83%), nearly always ideology-driven. With repeated DDoS claims against operators of railways, metros and tramways services, railway accounts for 32% of incidents in the sector.

CYBERCRIME ACTIVITIES



Incident type in cybercrime

Source: ENISA dataset

Ransomware

This kind of attacks continued disrupting operations, notably through data encryption. Fraud schemes, including business email compromises, payment diversions, scams and investment fraud, also remained widespread.

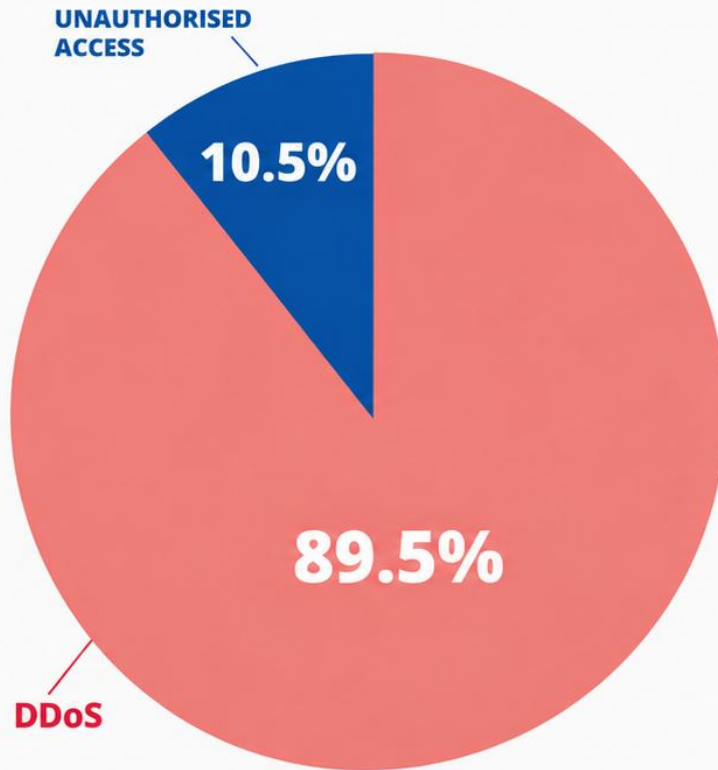


Data breaches continued to affect organisations across multiple sectors, exposing personal, financial, and corporate information that could be further exploited in criminal operations.



Multiple EU organisations were identified as targets of repeat victimisation, with activities, likely operationally linked and enabled by a lack of restoration practices following incident response.

HACKTIVIST ACTIVITIES



Incident type in hacktivism

Source: ENISA dataset

Hacktivism

ENISA recorded 4 709 hacktivist claims against EU MSs, of which more than 89% involved low-impact DDoS, notably driven by the geopolitical context. Activities were driven by several groups, particularly pro-Russia NoName057(16).

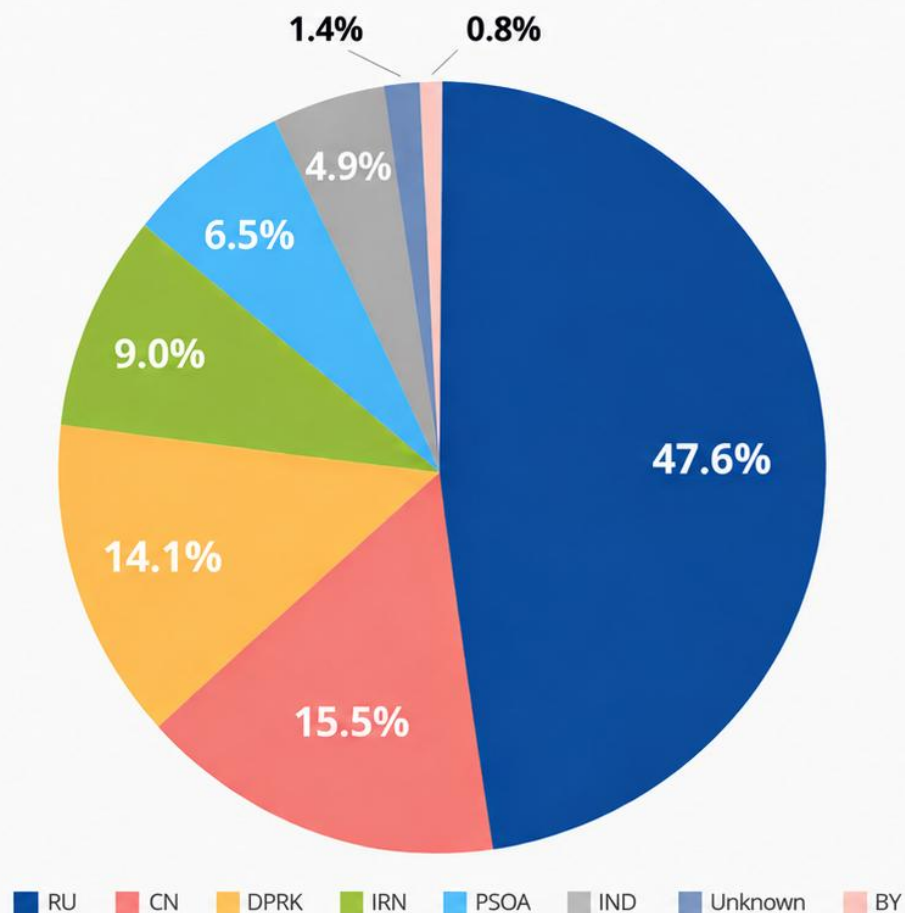


Hacktivism remains relevant as it combines disruption and intrusion claims with a FIMI component directly tied to political and societal events, ultimately resulting in **reputational and operational pressure** on public and private entities across the EU.



ENISA observed an increasing number of claims pertaining to the **targeting of Operational Technology**, notably by pro-Russia hacktivist groups.

STATE-NEXUS ACTIVITIES



State-nexus intrusion sets active in the EU by nexus

Source: ENISA dataset

State-nexus

Activities of State-nexus intrusion sets targeting EU MSs remained primarily focused on cyberespionage, and **strategic data collection**, notably through the compromise of digital infrastructure and the targeting of public administrations.



State-nexus activities in the EU continued being **prevalent against public administration (29.4%)**, followed by the targeting of manufacturing, digital infrastructure, civil society, and transport sectors.



State-nexus intrusion sets were seen continuing to leverage **tailored lures impersonating EU institutions, officials and affiliated entities**. 2025 saw the continued **targeting of EU entities outside EU territory**.

VULNERABILITIES

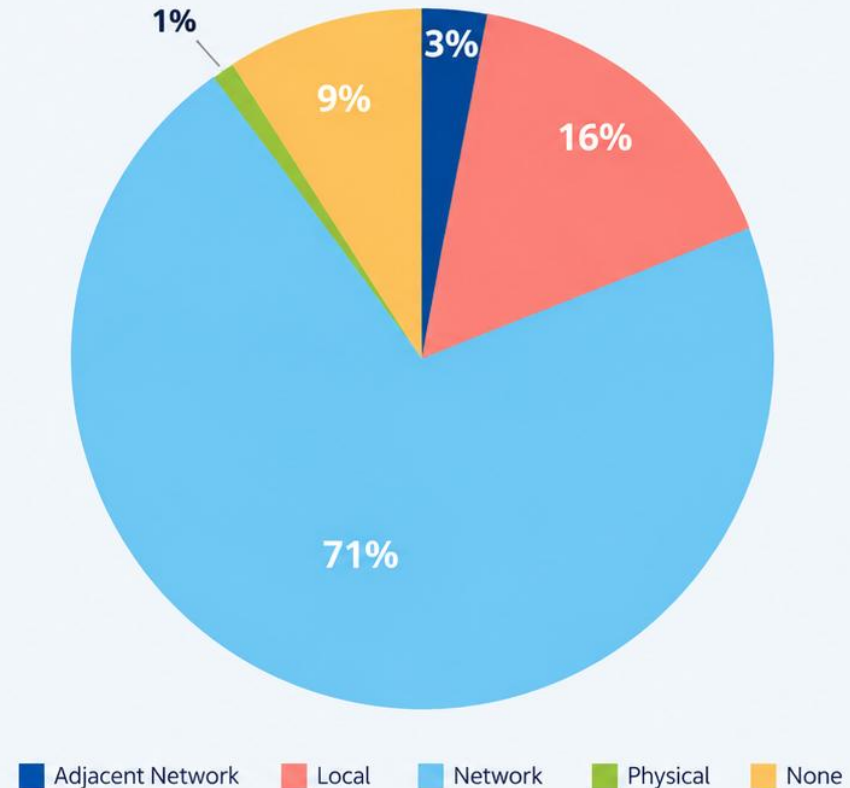
Vulnerabilities

Overall, more than
48 thousand
new vulnerabilities
were assigned a CVE number
and published in 2025 – a
22% increase
from the previous year.



When considering the attack surface, **71%** of documented vulnerabilities mentioned **Network** as the attack vector. This underscores the potential risk of remote exploitation, especially for internet-facing systems.

Attack vector in documented vulnerabilities
(2025)



Source: EUVD

Outlook

Current observations indicate that several of the dynamics documented during 2025 are likely to persist, shaping an increasingly complex and evolving cyber threat landscape for the EU.



Hacktivism will persist

Public and private organisations in EU MSs will continue to face hacktivist-associated threats, with periodic peaks, notably around high-visibility events and announcements by EU MSs and Union entities.



Stable cyberespionage activity

State-nexus intrusion sets, with a continued prevalence of Russia-nexus and China-nexus groups, are likely to maintain sustained activity, particularly targeting public administration and other high-value sectors.



Cybercrime remains a major threat

Cybercrime will highly likely remain one of the most impactful threats to business continuity. Extortion schemes and breaches will evolve, with displaced RaaS brands quickly replaced by emerging programmes, and an increasingly mature, fragmented and resilient ecosystem.



Convergence across threats

Operational practices across cybercriminal, hacktivist and State-nexus groups are likely to further converge, with similar vulnerabilities, platforms and toolsets used regardless of assessed objectives, complicating imputation and increasing the need to address common weaknesses.



Growing digital dependencies

Software suppliers, developers, managed service providers, cloud platforms and customer-service environments will remain high-value targets. Opportunities for threat groups to achieve broader impact through a single compromise are likely to increase.



AI as a force multiplier

AI is likely to further accelerate threat activity. While it will highly likely continue to primarily act as a force multiplier, 2026 may see an increased number of the kill chain's phases being directly enabled by AI, with possible experimentation of Human-out-of-the-loop proof of concepts.



Thank you for your attention

press@enisa.europa.eu

etl@enisa.europa.eu

ENISA

European Union Agency
for Cybersecurity

Athens Office

Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office

Rue de la Loi 107
1049 Brussels, Belgium