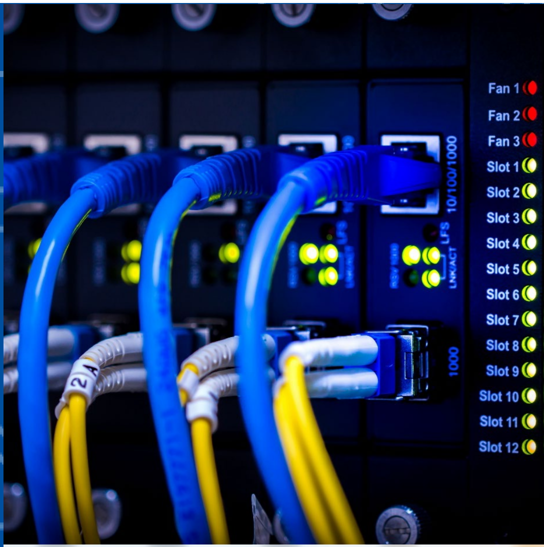
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

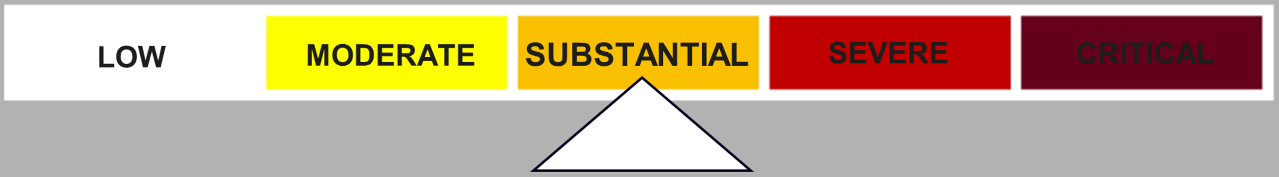
2024 TELECOMMUNICATIONS CYBER THREAT OVERVIEW



J. BOUTEMEUR, Head of Threat Analysis

20 | 03 | 2025

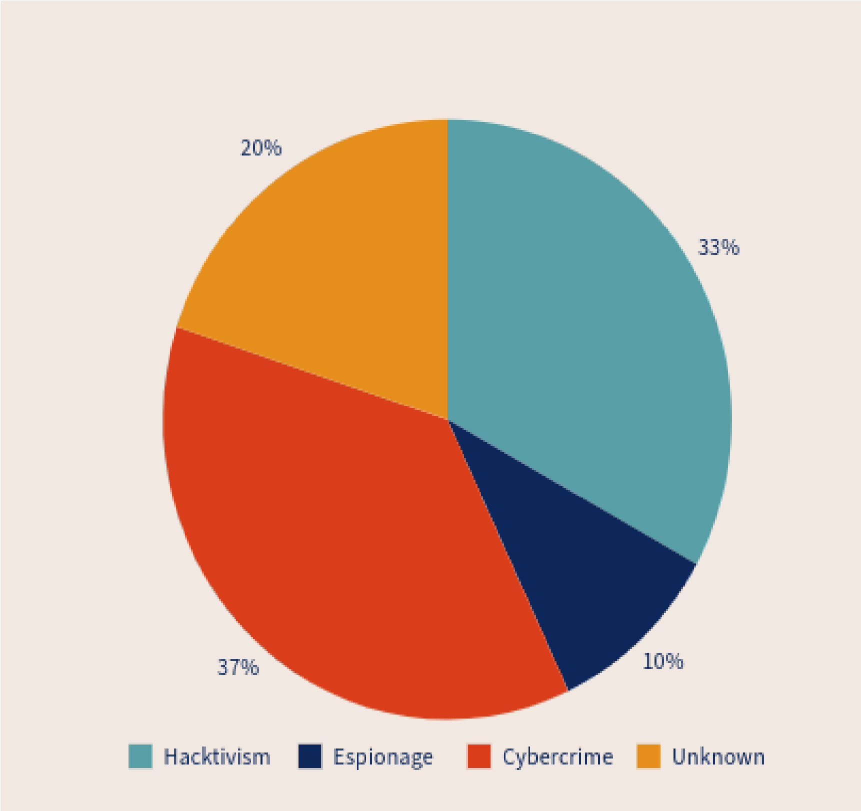
THREAT LEVEL



EU MS Telecom sector likely being directly targeted by threat actors or could be exposed to breaches using known and unknown vulnerabilities

THREAT LANDSCAPE

30 cybersecurity incidents in 2024



Source : ENISA OSINT collection

Hacktivism

- NoName057(16)
- Cyber Army of Russia Reborn (CARR)

Cybercrime

- Lockbit3.0
- Play
- RansomHub

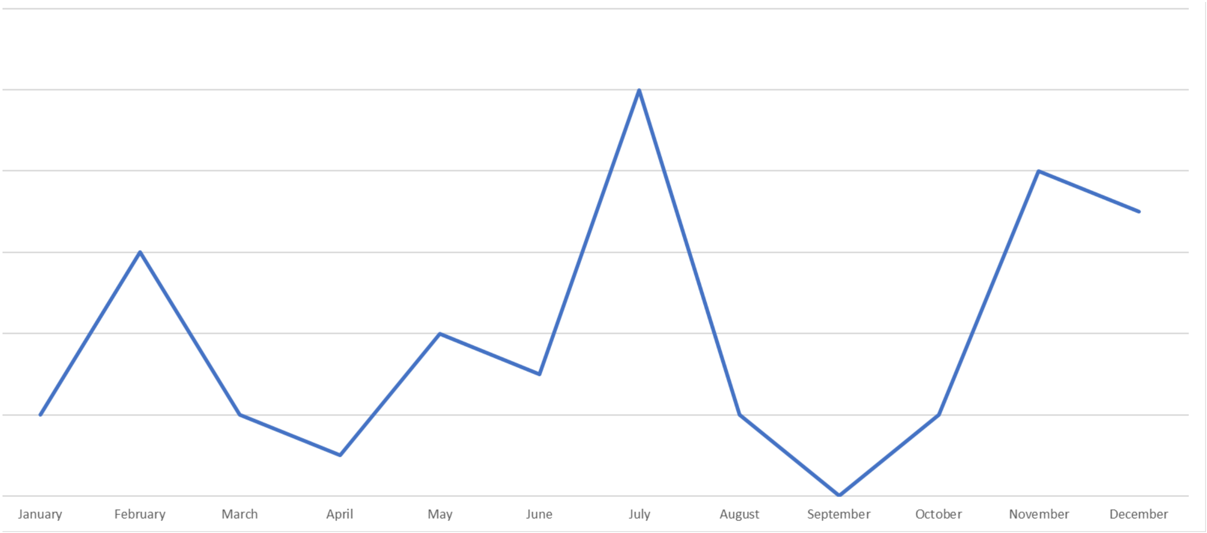
Cyberespionage

- APT29
- Salt Typhoon
- Earth Lusca
- Velvet Ant

TLP: GREEN

TEMPO OF ACTIVITY

Continuous targeting over the year, with a few spikes



Late January–February: Several attacks reported in SP, IT, NL, BE, and DK.

June–July: Uptick in attacks claimed by NoName057, focusing on RO, BE, FR, and PT.

November: Another cluster of incidents, mostly data breaches and ransomware, especially affecting FR and IT.

TLP: GREEN

EU NOTEWORTHY CYBER INCIDENTS

- **Edpnet – March 2024,**

ISP Edpnet suffered a cyberattack hindering customers access to their accounts.

- **Telefónica Data Breach – May 2024**

A database with 2.6 million records, affecting over 120,000 clients, was stolen and offered for sale on a dark web forum. The data included sensitive customer information such as names, phone numbers, and addresses.

- **SFR Data Breach – July/September 2024**

Telecom provider SFR suffered a breach of its customer order management system, exposing names, addresses, IBAN numbers, and SIM card details of 1.4 million customers.

- **Free Telecom Breach – October 2024**

Telecom provider Free was targeted in a data breach compromising customer information.

KEY OBSERVATIONS

- Direct targeting vs. leveraging of telco
- DDoS attacks grounded in geopolitical context
- Mid-term impact of data breaches & ransomware
- Hybrid operations

TLP: GREEN

OUTLOOK

- ⇨ Continuation of activities carried out by State-nexus, cybercrime and hacktivist intrusions sets.

- ⇨ Continuous exploitation of zero-day vulnerabilities + new attack vectors will emerge, including AI-driven phishing.

- ⇨ Third-party risk will remain critical.

TLP: GREEN

THANK YOU FOR YOUR ATTENTION

✉ tas@enisa.europa.eu

www.enisa.europa.eu