TLP:CLEAR

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA Threat Landscape 2026

SEPTEMBER 2026

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.

CONTACT

To contact the authors, please use etl@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

ENISA

ACKNOWLEDGEMENTS

EEAS STRATCOM

Europol

Automotive Information Sharing and Analysis Center (Auto-ISAC)

Aviation Information Sharing and Analysis Centre (Aviation ISAC)

European Top-Level Domain Information Sharing and Analysis Centre (European TLD ISAC)

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-807-5, DOI 10.2824/0806036

DISCLAIMER

AI was used in a limited capacity to support collection and processing of data used in this report. All outputs were reviewed and validated by subject-matter experts. No AI-generated content was used in this report. All references and external resources cited in this report were accessible at the time of publishing. ENISA cannot guarantee their continued availability and bears no responsibility for subsequent changes to, relocation of, or removal of content hosted by third parties. Where relevant, references to specific channels, forums, and Data Leak Sites (DLS) are provided for informational and evidentiary purposes. Such resources are inherently volatile and may become inaccessible, including as a result of deletion by their operators, account or infrastructure suspension, or law-enforcement action.

Table of Contents

Executive Summary 7

Methodology 9

1. Overview & Trends 11

2. Sectoral Analysis 18

2.1 Public administration 20
2.2 Business services 24
2.3 Transport 27
2.4 Manufacturing 31
2.5 Finance / Banking 34

3. Cybercrime Threats 38

3.1 Key threats 39
3.1.1 Fraud and Impersonation 39
3.1.2 Data breaches 42
3.1.3 Ransomware deployments 46
3.2 Sectoral impact 54
3.3 Geographical impact 54
3.4 Key trends 55
3.5 Tackling cybercrime in the EU 59

4. State-Nexus Threats 60

4.1 Key threats 60
4.2 Sectoral impact 67
4.3 Key TTPs and trends 69

5. Foreign Information Manipulation & Interference (FIMI) 74

5.1 Key threats 74

6. Hacktivist Threats 83

6.1 Key threats 83

6.2 Sectoral impact 85
6.3 Geographical impact 85
6.4 Key trends 88

7. Vulnerabilities 90

8. Outlook and Conclusion 95

Appendix A Law Enforcement Authorities operations in the EU 97

Appendix B Assessment methodology 100

Executive Summary

The 2025 cyber threat landscape affecting the European Union remained **shaped by a combination of threats, sometimes driven by geopolitical developments**, and the growing interconnectedness of digital ecosystems.

DDoS attacks (51.3%) and unauthorised access (39.5%) continued to account for a large share of the recorded activity affecting EU Member States and EU-based organisations. **Social engineering** remained a common enabling tactic to abuse trust, particularly through phishing campaigns (77.8%), increasingly supported by phishing kits and service-based ecosystems. The exploitation of **vulnerabilities**, including N-day and 0-day vulnerabilities, also remained a prevalent intrusion vector to enable unauthorised access (60.4%). At the same time, the targeting of supply chains, third-party providers, cloud environments and other **cyber dependencies** continued resulting in impactful and large-scale incidents.

Financially motivated activities (29.3% of all recorded incidents), particularly ransomware, remained the **most impactful incidents in the short-term**. Ransomware, data breaches, phishing and fraud impacted a broad range of sectors, reflecting the continuing adaptability of the cybercrime ecosystem. Manufacturing, business services and public administration were among the sectors most affected by cybercrime-related activities. Across the reporting period, ransomware operators continued relying on extortion and data exposure through public claims shared on Data Leak Sites (DLS) and dark web forums, while fraud and phishing activity highlighted the continued importance of credential compromise, impersonation and social engineering techniques, notably through the increased use of ClickFix and SMS phishing (smishing).

Geopolitical developments such as the continuation of Russia's war of aggression against Ukraine or the conflict escalation in the Middle East **continued influencing cyber activity impacting the EU**. Ideology-driven operations represented a significant share of the observed activity (57.3%), particularly through hacktivist-led DDoS campaigns targeting public-facing services, essential entities and organisations associated with political developments or support for countries such as Ukraine or Israel. State-nexus intrusion sets continued conducting cyberespionage activities (5.9%), with Russia-nexus intrusion sets primarily targeting central governmental and diplomatic entities, and China-nexus intrusion sets showing continuous interest in the transport sector including maritime related entities. A resurgence in State-nexus financially motivated campaigns was observed.

2025 confirmed the **continued exposure of sectors** to cyber threats, including sectors of high criticality according to NIS2. Public administration remained the most impacted sector (31.8%), followed by business services (8.5%), transport (8%), manufacturing (6.9%) and finance / banking (5.6%). Sectoral analysis further highlighted differences in targeting patterns, threat groups and operational impact across sectors, notably showing the criticality of digital dependencies, sensitive data holdings and operational maturity in shaping exposure to cyber threats.

Another notable development throughout the reporting period was the **continued adaptation of threat groups' operational playbooks**. Cybercriminal, hacktivist and State-nexus threat groups increasingly relied on scalable techniques, shared tooling patterns and trusted digital environments to conduct malicious activities. 2025 also observed the continued integration of **artificial intelligence** into malicious cyber activities, including activities carried out by cybercriminal operators, State-nexus intrusion sets and Information Manipulation Sets (IMS).

Looking ahead, ENISA assess that **several of the dynamics observed during 2025 are likely to persist** into the next reporting period. Organisations across the EU will continue facing a combination of cybercrime, cyberespionage and hacktivist activity driven by geopolitical developments. While objectives remain distinct, cybercriminal, hacktivist and State-nexus operators increasingly rely on

similar access vectors, tools and operational approaches, making imputation and threat analysis more challenging. Cybercrime is expected to remain one of the most significant sources of disruption to organisations operating in the EU, supported by mature criminal ecosystems, evolving extortion models and the continued availability of specialised services and tooling. The reporting period also reinforced the importance of digital dependencies, as incidents affecting software suppliers, service providers and cloud environments continued demonstrating the potential for broader downstream impact. **ENISA assess artificial intelligence will highly likely increasingly support malicious operations**, and its use will likely expand beyond the increased speed, scale and adaptability of cyber operations, **it is also likely 2026 will 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. The growing availability of frontier AI models and specialised malicious or dual-use tooling has already demonstrated its impact in augmenting the development of malicious capabilities and will likely lower barriers to entry into malicious cyber activities and further support scaling, automation and velocity across cyber operations. It is also likely that the use of these new models will increase EU organisations' exposure to new threats, arising from both accidental and malicious activities.

Methodology

The updated ENISA Cybersecurity Threat Landscape (ENISA CTL) methodology published in September 2026[1] was used to support the drafting of the ENISA Threat Landscape (ETL).

The ENISA Threat Landscape 2026 report is organised as follows. The first chapter provides an overview of the general threat landscape, highlighting specific trends considered relevant. The second chapter provides a sectoral overview of the incidents recorded in ENISA's dataset. The following chapters of this document provide a deep dive into four main areas, cybercrime, State-nexus activities, hacktivism, and Foreign Information Manipulation and Interference (FIMI). Incidents documented in the FIMI chapter were drawn from the European External Action Service's (EEAS) FIMI Threat Landscape 2025. A chapter is dedicated to the analysis of vulnerabilities disclosed during the reporting period, as well as an outlook to conclude this report.

For the ETL 2026 report, ENISA analysts collected and analysed **8 257 incidents**, mainly based on information from open sources, as well as anonymised information shared by EU Member States (EU MSs) and members of the ENISA Cyber Partnership Programme[2]. **The reporting period of the ETL has been updated to the calendar year**, i.e. the analysis takes into consideration incidents recorded from 1 January 2025 to 31 December 2025; hence, this report presents an overlap of six months with the previous ETL, presenting trends already described in the ETL2025.

For this ETL, ENISA also **expanded the number of tracked cybercrime activities** (including data breaches and fraud). While this was observed to have an impact on the numbers presented in this report, it did not substantially change the trends and rankings observed in the previous iteration. Of note, data breaches, frauds, scams and ransomware are expected to present overlaps (i.e. data exfiltrated through fraud schemes and ransomware deployments are advertised in forums, and data advertised in those forums are subsequently used in fraud schemes and ransomware deployments).

As much as possible, primary sources are referenced in footnotes to substantiate ENISA's assessments. ENISA appreciates that open sources and information shared voluntarily do not constitute a complete picture of the cyber threat landscape. Moreover, multiple caveats are inherent to open-source reporting. Those notably include **reporting granularity and temporality**. For instance, vague sectoral or geographic reporting (e.g. 'private companies', 'Europe') is likely to impact ENISA's dataset and analysis. Another caveat concerns proper sectoral categorisation, especially when one incident impacts an organisation operating in multiple sectors. To avoid inflating the threat, ENISA analysts undertook a thorough curation of the dataset either by choosing one specific sector or by registering the incident as 'unknown'. While particular attention was paid to the matter, it is highly likely a deviation will remain. Another example is the reporting of a specific number of targeted or impacted EU organisations in one report, whereas other reports will just mention the targeting of an EU MS. This notably affects the ranking of sectors and State-nexus intrusion sets. It should be noted that incidents are not necessarily reported immediately or confirmed in open sources. For instance, while ransomware and DDoS are more immediate 'visible' threats often claimed directly by their operators, cyberespionage campaigns are typically documented with a delay often spanning

[1] https://www.enisa.europa.eu/publications/enisa-cybersecurity-threat-landscape-methodology
[2] https://www.enisa.europa.eu/topics/cyber-threats/situational-awareness/enisa-cyber-partnership-programme-cpp

from six months to more than four years. It should also be noted that, to some extent, increased reporting of a specific threat does not necessarily reflect an increased tempo of activity but rather speaks to the audience's interest, particularly linked to a specific geopolitical context. Furthermore, while the number of hacktivist claims remain high, the threat of cyberespionage represents a more impactful threat in the long term.

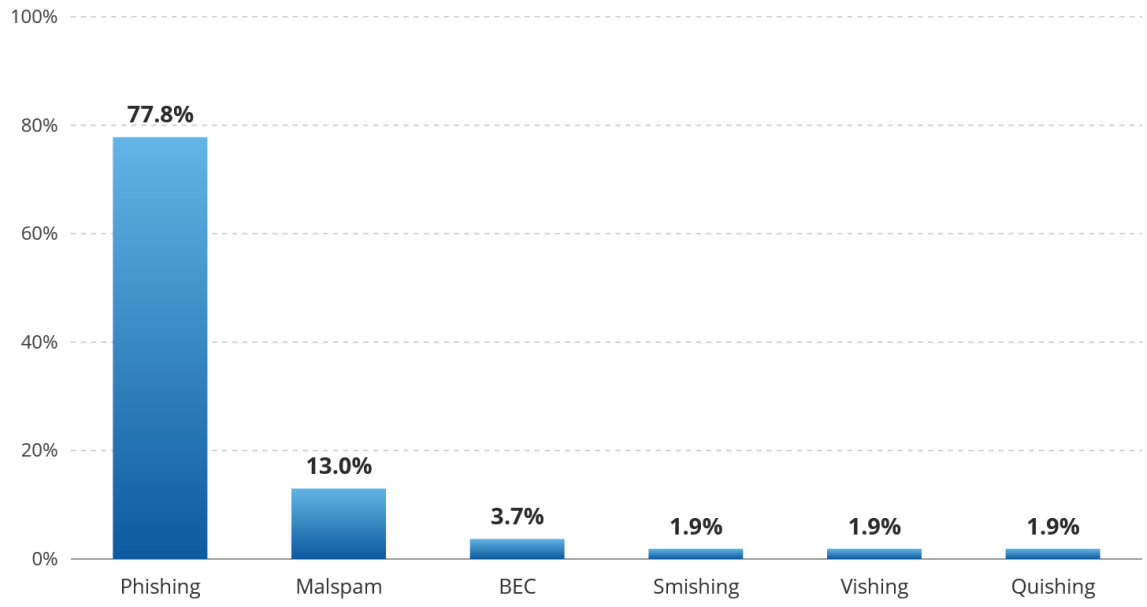
Hence, **this report should be seen as an overview of prevailing trends**, constituting a snapshot of threats faced by EU MSs and EU-based organisations.

To differentiate between what was reported by other sources and ENISA's own assessments, words of estimative probability are used, described within a matrix available in the Appendix.

1. Overview & Trends

Based on the analysis of the ENISA dataset, **DDoS remain the primary incident type (51.3%)**, followed by unauthorised access (39.5%). Among social engineering techniques, **phishing remains a prevalent intrusion vector** (77.8%), followed by malicious spam (malspam), accounting for 13%.

An **increasing use of the ClickFix technique**, abusing victim into 'fixing' an issue, ultimately leading to the execution of malicious code[3] [4], was prevalent in 2025. ENISA also observed the popularisation of phishing kits and Phishing-as-a-Service (**PhaaS**) platforms to further enable financially motivated cyber activities (see cybercrime threats chapter)[5] [6].



Source: ENISA dataset

Figure 1 - Social engineering techniques leveraged in identified incidents targeting the EU

Exploitation of N-day and 0-day vulnerabilities remains a prevalent intrusion vector. Across incidents of unauthorised access for which ENISA was able to identify an intrusion vector (5.2%), 60.4% were seen leveraging a vulnerability, while **misconfiguration and accidental exposure** remain a concern (20.7%). Unauthorised access by **insider threats contributed an increased share** compared to the previous ETL, likely due to the threat posed by Famous Chollima, an intrusion set associated to the Democratic People's Republic of Korea (DPRK)

[3] https://news.sophos.com/en-us/2025/12/18/i-am-not-a-robot-clickfix-used-to-deploy-stealc-and-qilin/
[4] https://www.proofpoint.com/us/blog/threat-insight/around-world-90-days-state-sponsored-actors-try-clickfix
[5] https://catalyst.prodaft.com/public/report/lucid/overview
[6] https://www.trellix.com/blogs/research/phaas-phishing-as-a-service-on-the-rise/

seeking employment as IT workers globally, including in EU companies, notably defence and government-related entities[7] [8] [9] (see State-nexus threats chapter).

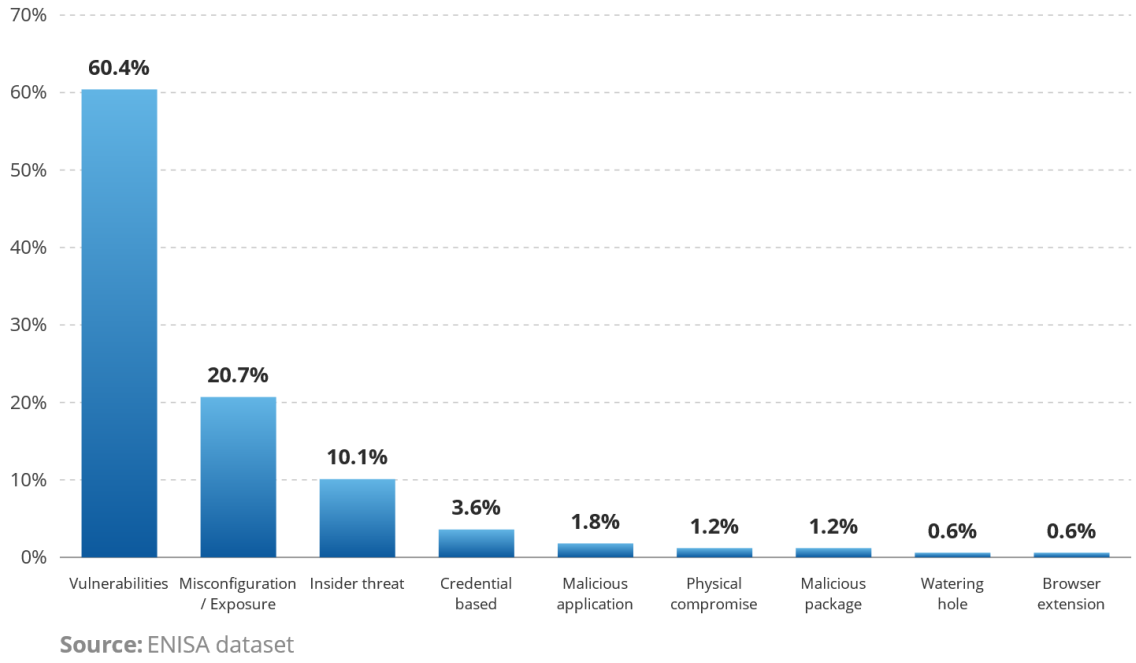


Figure 2 - Intrusion vectors observed in unauthorised access incidents in the EU

The **targeting of cyber dependencies**, including **supply-chain attacks and third-party attacks** continued to be observed, with several examples of large-scale and/or impactful incidents throughout the reporting period. Cybercriminals increasingly targeted third-party providers, such as digital services, highly likely as an opportunity to optimise the efficiency of their attacks[10] [11] [12] [13] [14].

Adversaries were also seen exploiting the digital supply chain, notably by compromising software, repositories or browser extensions[15] [16] [17] [18](see sectoral analysis, cybercrime and State-nexus chapters). Of particular concern was the increase in compromises of popular libraries or npm packages, as seen with the Shai-Hulud campaign[19] [20]. In March 2026, ENISA published a technical advisory for the secure use of package managers[21].

The distribution of incident types remains **dominated by low-impact DDoS attacks**, which make up 51.3% of all recorded incidents, primarily shaped by geopolitical developments and political

[7] https://cloud.google.com/blog/topics/threat-intelligence/dprk-it-workers-expanding-scope-scale
[8] https://www.crowdstrike.com/en-us/resources/reports/threat-hunting-report/
[9] https://go.crowdstrike.com/2026-global-threat-report.html
[10] https://news.sophos.com/en-us/2025/05/27/dragonforce-actors-target-simplehelp-vulnerabilities-to-attack-msp-customers/
[11] https://www.tribunatreviso.it/cronaca/mon-hacker-attacco-biglietti-xueo4que
[12] https://www.fsbusitalia.it/it/umbria/news-umbria/2025/4/9/comunicazione-di-una-violazione-dei-dati-personali-agli-interess.html
[13] https://www.bvg.de/de/unternehmen/medienportal/pressemitteilungen/2025-05-15-statment-it-angriff-dienstleister
[14] https://www.acn.gov.it/portale/documents/20119/923891/operational_summary_apr2025_CLEAR_EN.pdf
[15] https://socket.dev/blog/60-malicious-npm-packages-leak-network-and-host-data
[16] https://socket.dev/blog/north-korean-apt-lazarus-targets-developers-with-malicious-npm-package
[17] https://socket.dev/blog/lazarus-strikes-npm-again-with-a-new-wave-of-malicious-packages
[18] https://www.koi.ai/blog/4-million-browsers-infected-inside-shadypanda-7-year-malware-campaign
[19] https://www.trendmicro.com/en_gb/research/25/i/npm-supply-chain-attack.html
[20] https://www.trendmicro.com/en_gb/research/25/k/shai-hulud-2-0-targets-cloud-and-developer-systems.html
[21] https://www.enisa.europa.eu/sites/default/files/2026-03/ENISA%20Technical%20Advisory%20-%20Package_Managers_Final.pdf

statements. The second half of 2025 recorded an increased number of intrusion claims by hacktivist groups, notably pertaining to the targeting of **Operational Technology (OT)** (see hacktivist threats chapter). Unauthorised access follow with 39.5%, dominated by financially motivated activities (63.9%), followed by ideology driven claims (15.3%), and cyberespionage (13.6%).

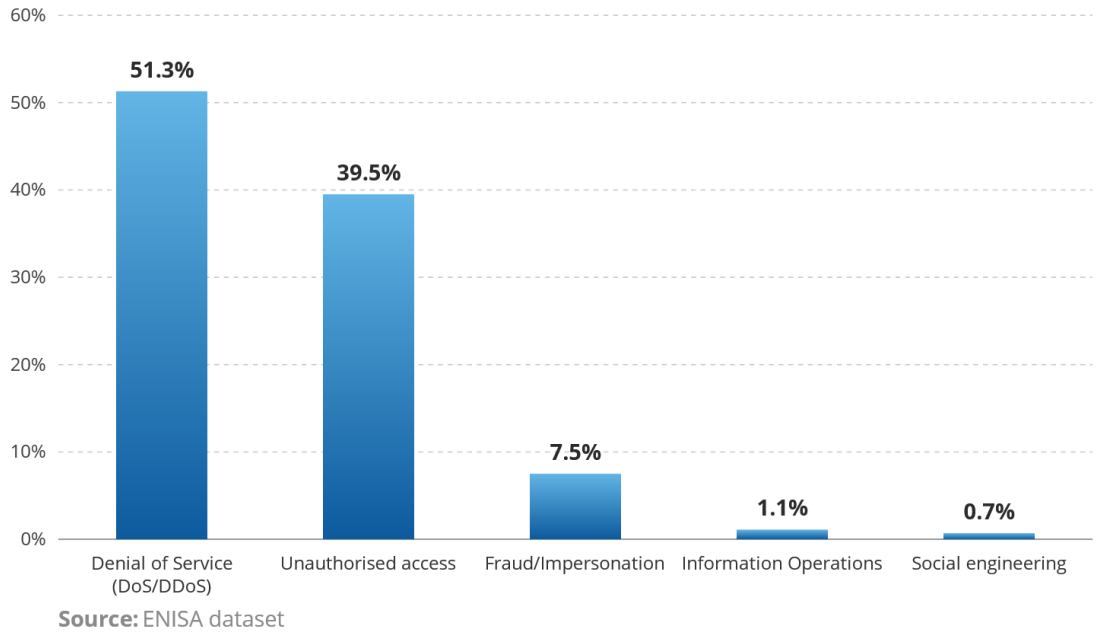


Figure 3 - Breakdown of incident types impacting the EU

Based on assessed objectives, **cyber activities targeting or impacting the EU mostly pertained to ideology-driven incidents** (57.3%), followed by financially motivated operations (29.2%). Cyberespionage campaigns accounted for 6.3%. As mentioned, despite representing most incidents, ideology-driven claims did not result in large-scale or significant impact. Though accounting for lower numbers, **financially motivated activities remain the most impactful threat to EU organisations in the short-term** and cyberespionage represents a significant strategic threat in the mid to longer-term. This is also reflected in ENISA's NIS investments report[22], where DDoS are characterised as 'noise' by representatives of EU organisations operating in NIS sectors of high criticality, while ransomware dominate organisational concerns.

[22] https://www.enisa.europa.eu/publications/nis-investments-2025

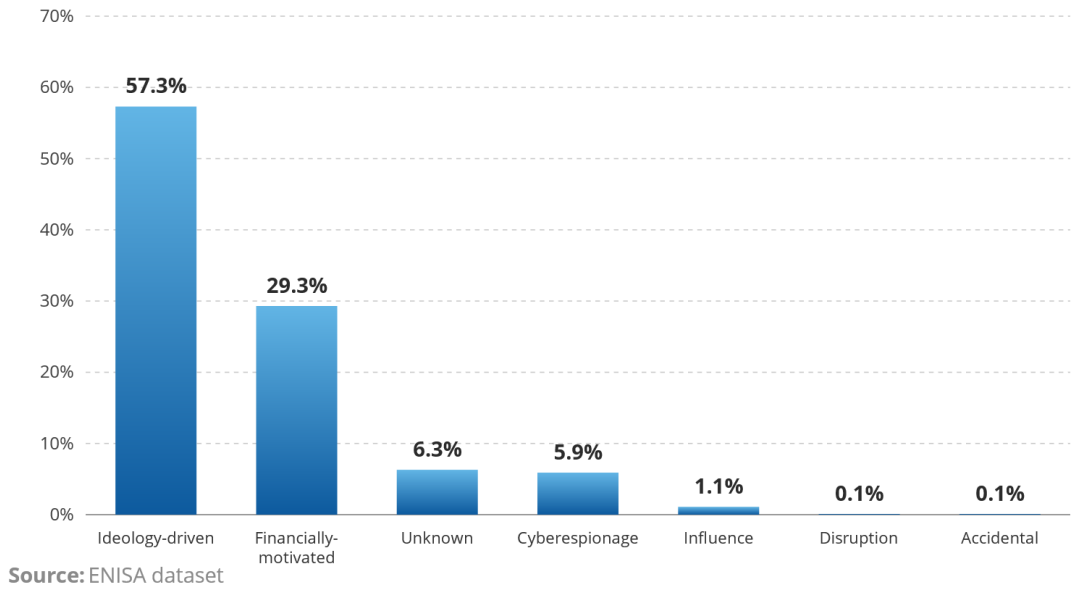
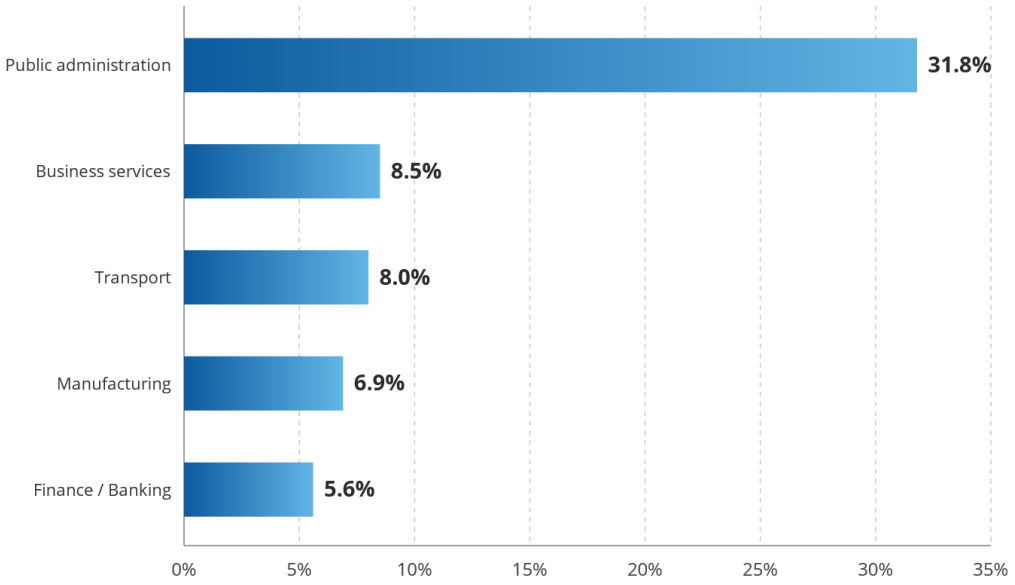


Figure 4 - Breakdown of incidents by assessed objectives

As already flagged in ETL 2025, the **distinction between threat categories continued to blur**. Similar techniques, infrastructures and access mechanisms appeared repeatedly across cybercrime, hacktivist and State-nexus reporting, despite differences in underlying objectives. This was notably exemplified by hacktivist-led DDoS waves by pro-Russia groups around electoral events and geopolitical developments, where increased activity was often observed as typical FIMI-aligned behaviour to associate disruption with aspects of information operations (see hacktivist threats chapter). Another illustration is the **leveraging of cybercrime tradecraft or toolsets** such as ransomware and infostealers **by State-nexus intrusion sets**, as seen with Moonstone Sleet's use of the Qilin ransomware [23] [24] [25] (see State-nexus threats chapter).

The **top five targeted sectors** in the EU include public administration (31.8%), business services (8.5%), transport (8%), manufacturing (6.9%) and finance/ banking (5.6%), with essential entities representing 72.9% of the total number of recorded incidents. As in the previous ETL report, public administration remains the most targeted sector, with the threat picture **largely impacted by ideology-driven DDoS attacks** (see sectoral and hacktivism chapters).

[23] https://x.com/MsftSecIntel/status/1897738961348374621
[24] https://go.cyberproof.com/hubfs/CyberProof_MidYear_Cyber%20Threat%20Landscape%20Report.pdf
[25] https://services.google.com/fh/files/misc/m-trends-2025-en.pdf



Source: ENISA dataset

Figure 5 - Top 5 impacted / targeted sectors in the EU

ENISA continued to observe an increasing use of **Artificial Intelligence (AI)** by malicious cyber threat groups, including cybercriminals, State-nexus and Information Manipulation Sets (IMS), primarily to facilitate or enhance their activities to optimise the speed and success rates of their operations overall. The integration of AI systems into enterprise environments creates a new attack surface. Threat groups, including State-nexus intrusion sets, IMS and cybercriminals demonstrate consistent interest in AI systems both as tools to facilitate malicious activity and as targets for exploitation[26] [27] [28] [29] [30] [31] [32] [33]. Despite this activity, reporting over 2025 indicates that attackers primarily use consumer-grade AI tools to augment existing skills and adapt attack vectors rather than to achieve breakthrough capabilities.

While attackers primarily use AI to augment existing skills, model improvements have already been seen accelerating vulnerability discovery and exploitation. In 2025, Frontier AI labs continued to assess that threat groups are primarily leveraging closed AI models to augment existing skills rather than achieve novel breakthrough capabilities[34] [35]. Prior efforts spanned basic applications such as the use of LLMs to craft and distribute tailored phishing messages at scale, develop text and media for deployment in influence campaigns and generate synthetic identities for remote-worker schemes[36] [37] [38]. Threat groups continue to experiment with methods for bypassing closed model

[26] https://www.group-ib.com/blog/the-dark-side-of-automation-and-rise-of-ai-agent/
[27] https://www.sentinelone.com/labs/akirabot-ai-powered-bot-bypasses-captchas-spams-websites-at-scale/
[28] https://www.trendmicro.com/en_us/research/25/c/ai-assisted-fake-github-repositories.html
[29] https://www.phonely.ai/blogs/how-does-ai-voice-cloning-work
[30] https://www.europol.europa.eu/cms/sites/default/files/documents/vishing_final_version.pdf
[31] https://www.security.com/threat-intelligence/malware-ai-llm
[32] https://research.checkpoint.com/2025/funksec-alleged-top-ransomware-group-powered-by-ai/
[33] https://www.sentinelone.com/blog/blackmamba-chatgpt-polymorphic-malware-a-case-of-scareware-or-a-wake-up-call-for-cyber-security/
[34] https://cdn.openai.com/threat-intelligence-reports/7d662b68-952f-4dfd-a2f2-fe55b041cc4a/disrupting-malicious-uses-of-ai-october-2025.pdf
[35] https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools
[36] https://www.ic3.gov/PSA/2026/PSA260521
[37] https://www.bbc.com/news/articles/cx2r7grrdwzo
[38] https://www.silentpush.com/blog/unmasking-the-dprk-remote-worker-problem/

safeguards and constraints, including steganography and indirect prompt injection[39] [40] [41] [42]. 2025 also saw the development of more industrialised methods for ensuring reliable, affordable and anonymised access to premium LLM tiers. The reporting period saw further proliferation of likely AI-generated malware leveraged in real-world operational contexts, as seen with an LLM-produced sample reportedly exploiting the React2Shell vulnerability[43]. AI was also used to conduct reconnaissance, script development and post-exploitation, often supported by 'turnkey' AI-assisted toolkits resold via underground marketplaces[44] [45] [46].

Another relevant trend to highlight throughout the reporting period includes the **increased abuse of messaging applications and the leveraging of device code phishing** by multiple intrusion sets[47] [48] [49] [50] [51] [52] [53]. 2025 saw large scale campaigns targeting multiple EU MSs and sectors leveraging trusted communications platforms such as Signal or WhatsApp to initiate personalised contact and steering targets toward authentication through legitimate workflows to gain full access to compromised devices[54].

[39] https://cloud.google.com/blog/topics/threat-intelligence/ai-vulnerability-exploitation-initial-access
[40] https://www.microsoft.com/en-us/security/blog/2026/03/12/detecting-analyzing-prompt-abuse-in-ai-tools/
[41] https://www.miggo.io/post/weaponizing-calendar-invites-a-semantic-attack-on-google-gemini
[42] https://labs.zenity.io/p/agentflayer-chatgpt-connectors-0click-attack-5b41?
[43] https://www.darktrace.com/blog/ai-llm-generated-malware-used-to-exploit-react2shell
[44] https://www.sophos.com/en-us/blog/pointing-a-cursor-at-evading-detection
[45] https://www.sysdig.com/blog/ai-agent-at-the-wheel-how-an-attacker-used-llms-to-move-from-a-cve-to-an-internal-database-in-4-pivots
[46] https://www.sophos.com/en-us/blog/ai-in-the-underground-curiosity-claims-and-concerns
[47] https://www.volexity.com/blog/2025/02/13/multiple-russian-threat-actors-targeting-microsoft-device-code-authentication/
[48] https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/
[49] https://www.volexity.com/blog/2025/04/22/phishing-for-codes-russian-threat-actors-target-microsoft-365-oauth-workflows/
[50] https://blog.sekoia.io/apt28-operation-phantom-net-voxel/
[51] https://cloud.google.com/blog/topics/threat-intelligence/russia-targeting-signal-messenger/
[52] https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai
[53] https://cloud.google.com/blog/topics/threat-intelligence/ai-vulnerability-exploitation-initial-access
[54] https://www.microsoft.com/en-us/security/blog/2025/01/16/new-star-blizzard-spear-phishing-campaign-targets-whatsapp-accounts/

AI THREAT

While outside the reporting period, ENISA cannot overlook the evolution and emergence of advanced AI models in 2026, which have already shaped the threat landscape, notably through Proof of Concept (PoC) research related to AI-powered malware, and the first signs of malware using generative AI at runtime[55]. The most established trend remains the **use of AI to support and accelerate existing techniques** leveraged by malicious operators. Microsoft reported the operationalisation of AI by threat groups across different stages of cyber activity[56], while Anthropic reported that a state-nexus group used an agentic AI system during a campaign against unidentified international targets, with a limited number of successful compromises[57].

AI continued to be reported for phishing, fraud and malware development, including through impersonation of legitimate AI services. A fake Claude AI website, for example, was used to distribute malware[58], while cybercriminal forums continued discussing generative AI for phishing, fraud and malware development[59]. Analysis of the Gentlemen ransomware group, particularly active in the EU, also documented how their operators used AI coding assistants to develop the group's Ransomware-As-A-Service (RaaS) panel[60]. Of particular interest is the potential for AI to **increase the speed and scale of cyber malicious operations**. An AI-assisted cloud intrusion reportedly achieved administrative access within 8 minutes[61]. AI-assisted discovery and living-off-the-land activity has also been reported[62]. This reinforces concerns around faster PoC development, scanning and **vulnerability exploitation**. Reporting also shows AI becoming **more directly integrated into attack workflows**, as illustrated with the "AI in the Middle" technique, demonstrating how web-based AI services could potentially be abused to ensure **stealthy** operations **and resilience** of adversary infrastructure[63]. AI-linked developer environments and **software supply chains** are another area of concern[64] [65]. **AI applications and their ecosystems are increasingly becoming targets**, particularly where they have access to files, credentials, browser sessions or development environments[66] [67] [68] [69], and AI services may also provide a path into trusted environments[70] [71].

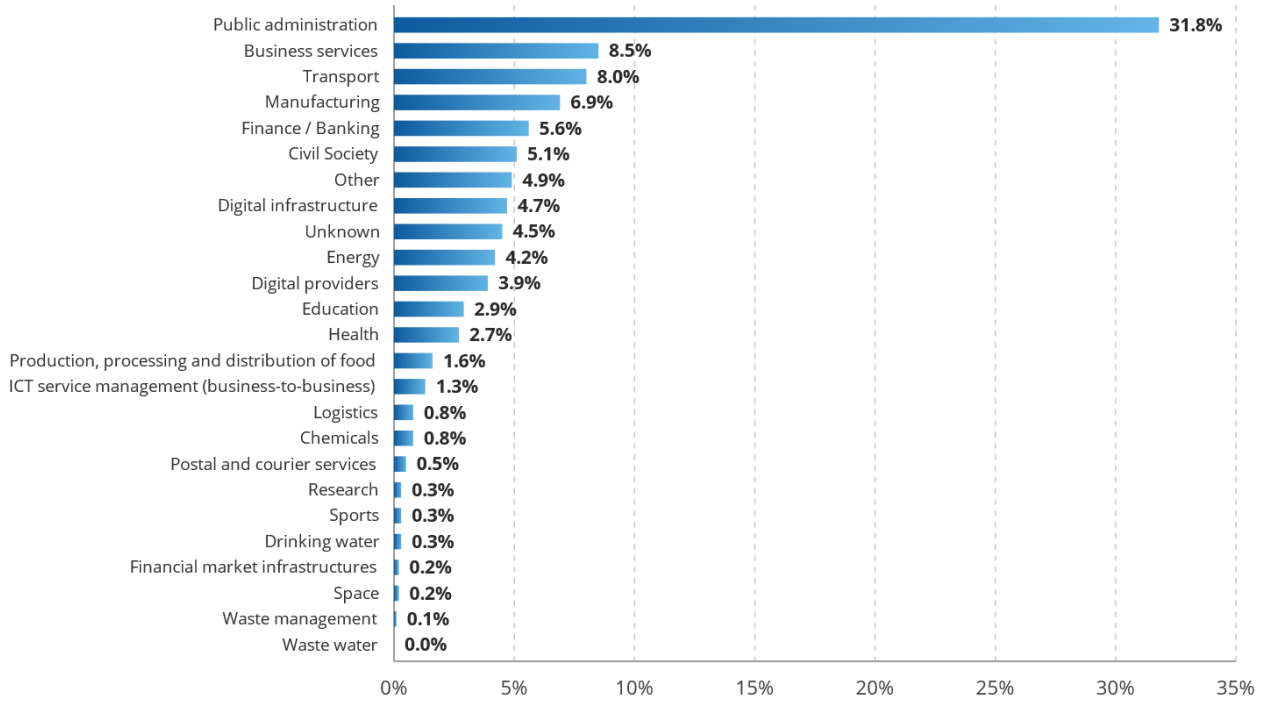
In this context, the European Commission published their EU Action Plan on Cybersecurity and Artificial Intelligence[72], building on the AI Act, the Cyber Resilience Act, NIS 2 and the Cyber Solidarity Act, to address cybersecurity risks and opportunities linked to Artificial Intelligence. On the same day, ENISA published their view on cybersecurity in the Frontier AI Era to provide a set of recommendations when developing operational capabilities[73].

[55] https://www.welivesecurity.com/en/eset-research/promptspy-ushers-in-era-android-threats-using-genai/
[56] https://www.microsoft.com/en-us/security/blog/2026/03/06/ai-as-tradecraft-how-threat-actors-operationalize-ai/
[57] https://www.anthropic.com/news/disrupting-AI-espionage
[58] https://www.malwarebytes.com/blog/scams/2026/04/fake-claude-site-installs-malware-that-gives-attackers-access-to-your-computer
[59] https://www.sophos.com/en-us/blog/ai-in-the-underground-curiosity-claims-and-concerns
[60] https://socradar.io/blog/gentlemen-ransomware-leak/
[61] https://www.sysdig.com/blog/ai-assisted-cloud-intrusion-achieves-admin-access-in-8-minutes
[62] https://cloud.google.com/security/report/resources/cloud-threat-horizons-report-h1-2026
[63] https://research.checkpoint.com/2026/ai-in-the-middle-turning-web-based-ai-services-into-c2-proxies-the-future-of-ai-driven-attacks/
[64] https://fieldeffect.com/blog/field-effect-detects-amos-stealer-delivered-via-cursor-ai-agent-session
[65] https://expel.com/blog/inside-lazarus-how-north-korea-uses-ai-to-industrialize-attacks-on-developers/
[66] https://www.greynoise.io/blog/threat-actors-actively-targeting-llms
[67] https://www.pillar.security/blog/operation-bizarre-bazaar-first-attributed-llmjacking-campaign-with-commercial-marketplace-monetization
[68] https://www.microsoft.com/en-us/security/blog/2026/03/05/malicious-ai-assistant-extensions-harvest-llm-chat-histories/
[69] https://www.bleepingcomputer.com/news/microsoft/microsoft-says-bug-causes-copilot-to-summarize-confidential-emails/
[70] https://vercel.com/kb/bulletin/vercel-april-2026-security-incident
[71] https://www.infostealers.com/article/breaking-vercel-breach-linked-to-infostealer-infection-at-context-ai/
[72] https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1544
[73] https://www.enisa.europa.eu/publications/enisas-view-on-cybersecurity-in-the-frontier-ai-era

2. Sectoral Analysis

This chapter provides a sectoral analysis of incidents identified by ENISA, looking at how cyber activity has impacted sectors covered by the NIS2 Directive[74], as well as additional categories needed to capture relevant activity outside the strict scope of NIS2. Where relevant it is compared with other reports, including reporting by EU MSs under the NIS2 Directive as well as ENISA's NIS360 report, to identify targeting patterns and assessments[75].

The top five targeted sectors in the EU include **public administration (31.8%), business services (8.5%), transport (8%), manufacturing (6.9%) and finance/ banking (5.6%).** While recorded events include non-NIS2 sectors, **essential and important entities represent 73% of the total number of recorded events,** confirming the relevance of the NIS2 approach[76]. In this context, ENISA published their NIS2 technical implementation guidance to ultimately support a common cyber defence posture across the EU for concerned entities[77].



Source: ENISA dataset

Figure 6 - Distribution of identified incidents in the EU per sector

[74] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02022L2555-20221227
[75] https://www.enisa.europa.eu/sites/default/files/2026-05/ENISA%20NIS360%202026.pdf
[76] https://ciras.enisa.europa.eu/
[77] https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

To complement the open-source-based reporting, figure 7 presents the sectoral distribution of events reported by EU MSs under NIS2 for 2025[78] [79] [80]. Based on the latter, the top five affected sectors include public administration, health, digital infrastructure, banking and transport. Overall, **malicious actions accounted for the largest share of reported root causes across the most impacted sectors**. Public administration appeared as the most affected sector in both cases, while transport and banking/finance were also present among the top five. However, health and digital infrastructure appeared among the top five sectors in Member State reporting. These discrepancies notably stem from different scopes, thresholds and reporting conditions.

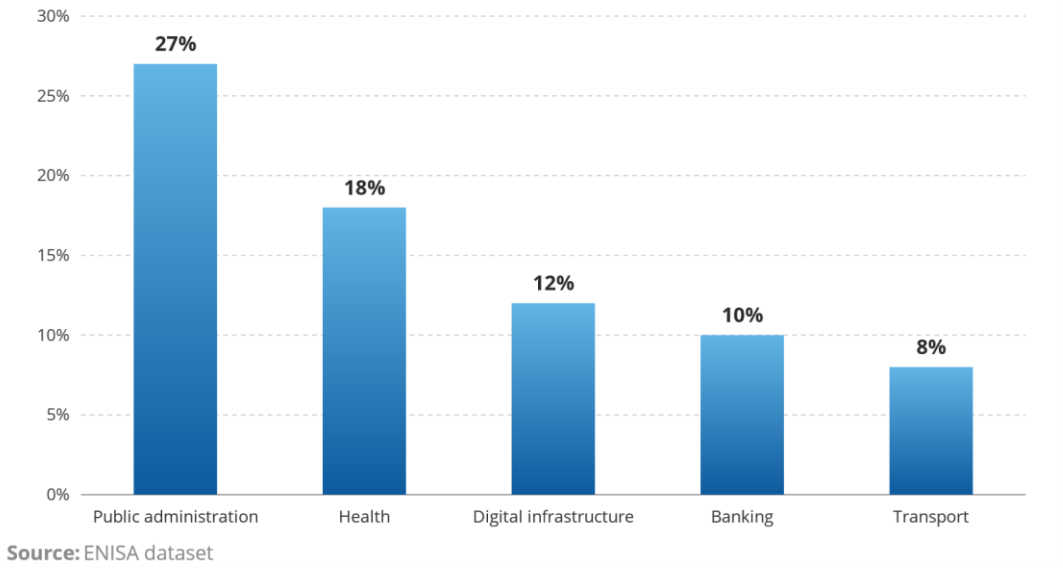


Figure 7 - Events reported by EU MS for 2025 under NIS2, per sector

[78] NIS2 requires EU MS to report notifications concerning incidents, cyber threats and near misses on a voluntary basis by essential and important entities, as well as other entities regardless of whether they fall in scope of NIS2. The term event is used for information reported by EU MS under NIS2 to refer to significant incidents, incidents, cyber threats and near misses.
[79] In 2025 and as to the 14th of July 2026, a total of 1 954 events were reported under NIS2. "Malicious actions" accounted for 941 events, for which around 50% the root cause was reported as unknown.
[80] https://ec.europa.eu/newsroom/dae/redirection/document/132389

2.1 Public administration

As in the previous ETL, public administration remains the **most targeted sector, accounting for 31.8%** of all recorded events. The distribution of incidents affecting public administration over the reporting period shows that **events primarily impacted central** (35.1%) and **local entities** (33.8%). Regional level entities accounted for 10.1% of events. Based on the ENISA NIS360 report, the EU public administration sector remains in the cyber risk zone, where criticality exceeds observed cybersecurity maturity.

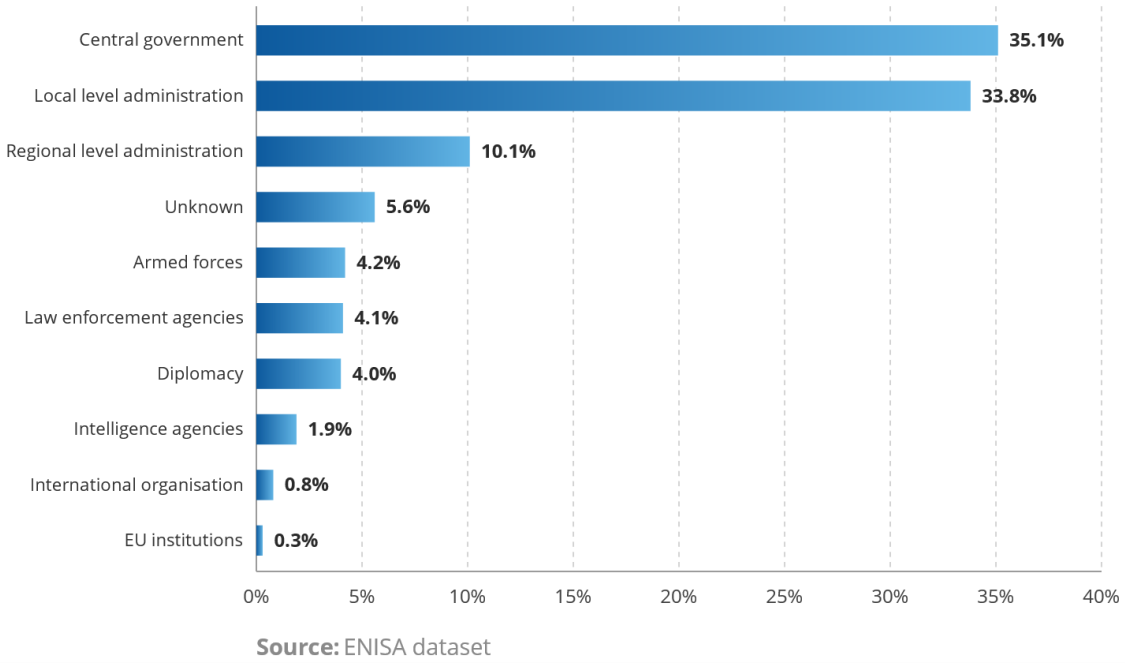


Figure 7 - Incidents impacting the EU public administration sector per sub-sector

The threat picture **is largely impacted by ideology-driven DDoS attacks which accounted for 81.8%** of the recorded incidents (see hacktivist threats chapter). Public-facing websites and portals of public administration entities were **repeatedly targeted around specific events**, such as law-enforcement takedowns and arrests, electoral processes, high visibility events and general geopolitical tensions including Russia's war of aggression against Ukraine and developments linked to the ongoing conflicts in the Middle East[81] [82].

[81] https://www.eurojust.europa.eu/news/hacktivist-group-responsible-cyberattacks-critical-infrastructure-europe-taken-down
[82] https://danish-presidency.consilium.europa.eu/en/news/european-council-adopts-conclusions-to-provide-90-billion-to-ukraine-over-the-next-two-years/

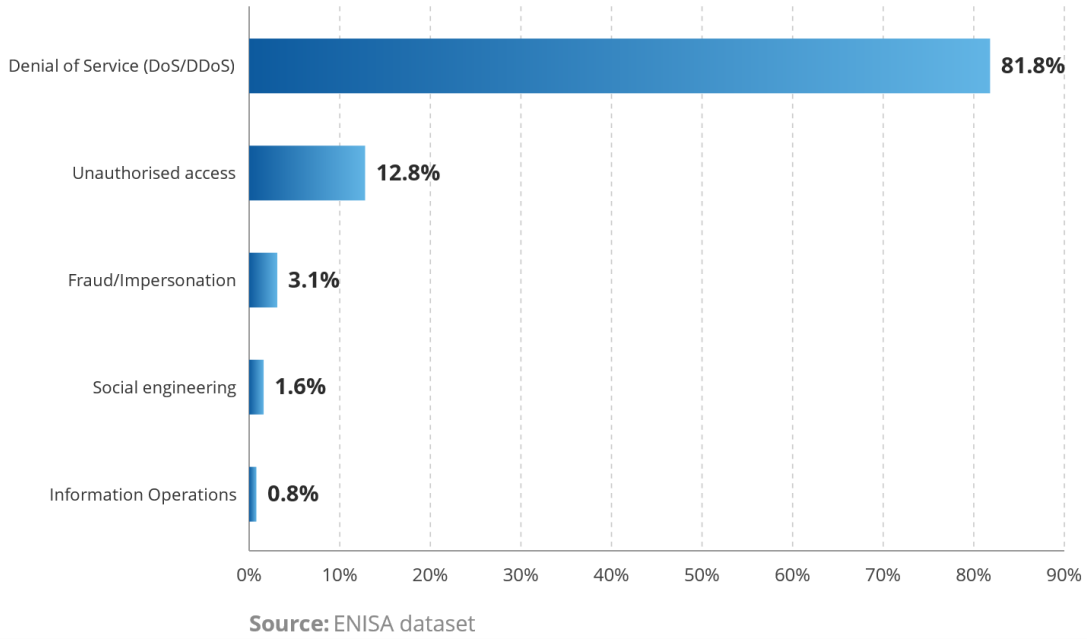


Figure 8 – Incident types impacting the EU public administration sector

NoName057(16), Dark Storm Team, and Mr. Hamza were the most active hacktivist groups targeting public administration in the EU (see hacktivist threats chapter). Groups such as Keymous+ and Server Killers further contributed to the sustained tempo of claimed DDoS attacks targeting the websites and web portals of public administrations in EU MSs, in the context of Russia's war of aggression against Ukraine. Other claims made by these alliances targeted public services, including visa and migration-related portals, as well as government targets framed by the groups as support for EU domestic protest movements. The reported impact remained largely limited to claimed or temporary disruption of public-facing websites[83] [84] [85].

[83] https://blog.cloudflare.com/ddos-threat-report-2025-q3/
[84] https://www.zataz.com/des-pirates-pro-russes-revendiquent-des-perturbations-en-soutien-au-10-septembre/
[85] https://cert.europa.eu/publications/threat-intelligence/cb25-10/

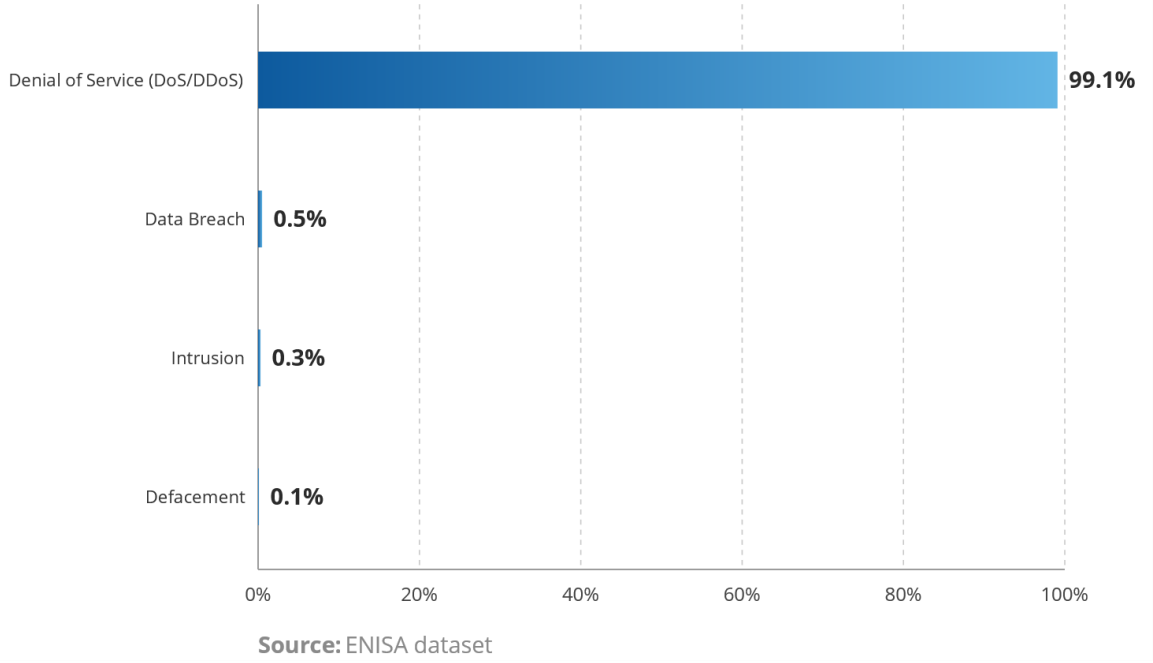


Figure 9 - Ideology driven claims against public administration in the EU

Among financially motivated incidents (8%) impacting the public administration sector in the EU, **ransomware claims accounted for 36%, primarily affecting municipalities** (see cybercrime chapter). The most deployed strains against the EU public administration sector included **Qilin, followed by SafePay and Stormous**. Despite their limited share, **several ransomware-related incidents resulted in operational disruptions**. A notable example was the ransomware attack against a Swedish IT supplier, which affected around 200 municipalities and regional authorities and disrupted systems used for HR reporting[86] [87]. Data breaches affecting the EU public administration sector accounted for 38.4%. Observed cases included the Pajemploi/URSSAF data theft in France, potentially affecting 1.2 million individuals, unauthorised access to a Slovenian public administration system exposing the records of 873 201 individuals, and a breach affecting several municipalities through an external appointment-service provider, reportedly exposing the data of around 100 000 individuals[88] [89] [90].

[86] https://therecord.media/sweden-municipalities-ransomware-software
[87] https://www.blt.se/karlskrona/cyberattack-mot-karlskronaforetag-utpressas-pa-pengar
[88] https://iledefrance.urssaf.fr/accueil/actualites/pajemploi-desormais-accessible-2.html
[89] https://www.gov.si/novice/2025-11-06-nepooblascen-vstop-v-informacijski-sistem-uprave-za-varno-hrano-veterinarstvo-in-varstvo-rastlin/
[90] https://france3-regions.franceinfo.fr/bretagne/finistere/quimper/vol-massif-de-donnees-en-bretagne-au-moins-cinq-communes-touchees-l-enquete-s-accelere-voici-ce-que-l-on-sait-3252205.html

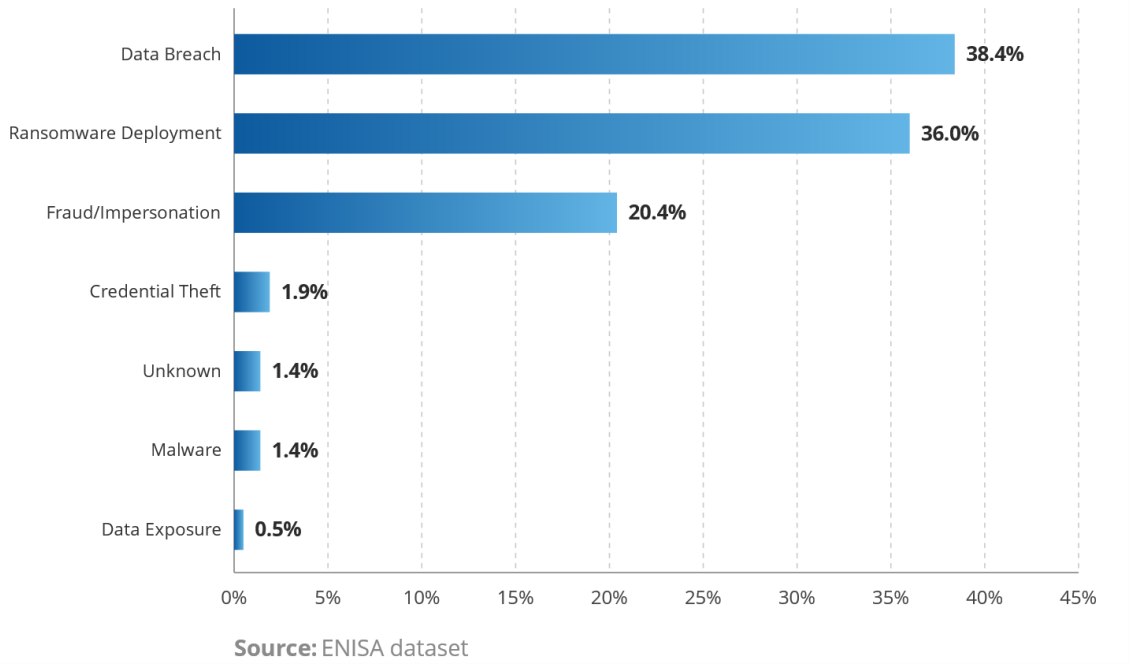


Figure 10 - Financially motivated claims against EU public administration

State-nexus intrusion sets targeting the public administration in the EU showed a **sustained focus on diplomatic and governmental entities for cyberespionage purposes**. Multiple intrusion sets were reported to be targeting a broader set of public administration organisations, including diplomatic entities, ministries, law enforcement agencies, political parties and core government institutions, as seen with Russia-nexus **APT29** targeting diplomatic entities in the EU, or activities associated with **APT28**, **Turla**, and **GoldenJackal**[91] [92] (see State-nexus chapter).

[91] https://cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-007/
[92] https://research.checkpoint.com/2025/apt29-phishing-campaign/

2.2 Business services

The business services sector was the **second most impacted sector in the EU (8.45%)**, primarily impacted by unauthorised accesses (56.7%), followed by DDoS attacks (38%). Among recorded unauthorised accesses against business services organisations, ransomware deployments accounted for 54%, followed by data breaches (26.5%).

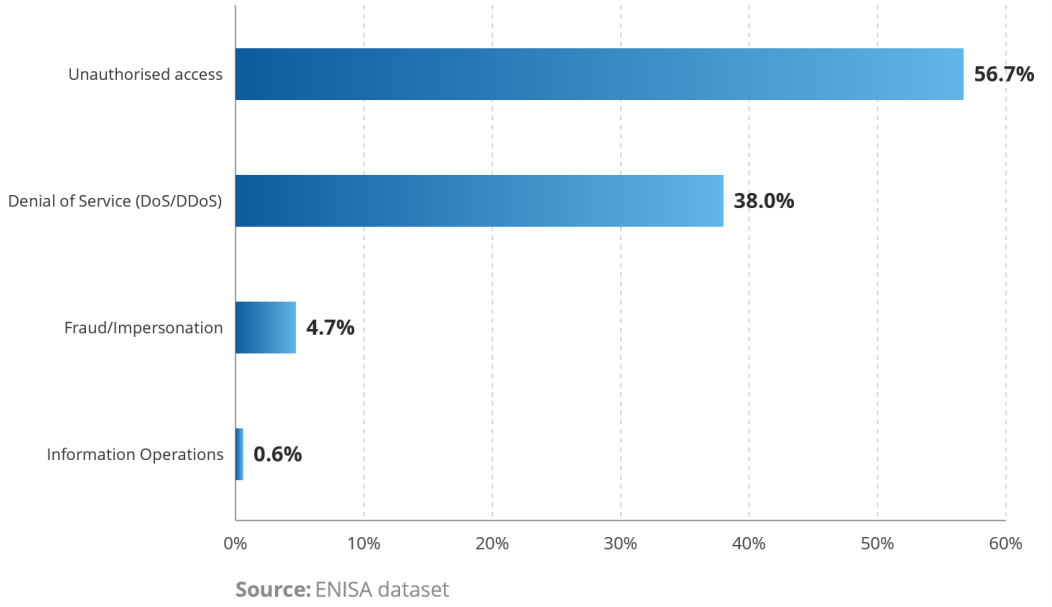


Figure 11 - Incident types impacting the EU business services sector

The business services sector captures a broad set of entities that fall outside the scope of the NIS2 Directive, notably including consultancy firms, legal services, broadcast media, real estate services and other professional or commercial service providers. **Hospitality, consultancy and broadcast media together accounted for 55.3% of events impacting business services**, showing that the sector's heterogeneous profile was partly shaped by concentrated activity in three highly visible subsectors.

Hospitality entities were impacted by several types of incidents, including DDoS attacks, ransomware claims and data breaches, as illustrated by a data breach impacting a Polish travel agency[93], whereas broadcast media was mostly impacted by hacktivist-led disruptions against public-facing communication platforms, as seen in the targeting of a Lithuanian public broadcaster's news website[94]. A ransomware incident against a French wealth management software provider showed the cascading effects of attacks against specialised services providers, with disruption reportedly affecting banks and wealth advisers for several days [95].

[93] https://www.brinztech.com/breach-alerts/brinztech-alert-polish-travel-giant-itaka-breached-2-2m-customer-records-pii-hashed-passwords-sold/
[94] https://www.lrt.lt/en/news-in-english/19/2503154/lrt-lt-suffered-cyber-attack-operations-not-disrupted
[95] https://www.clubic.com/actualite-556824-une-cyberattaque-majeure-paralyse-les-banques-et-conseillers-patrimoniaux-depuis-10-jours.html

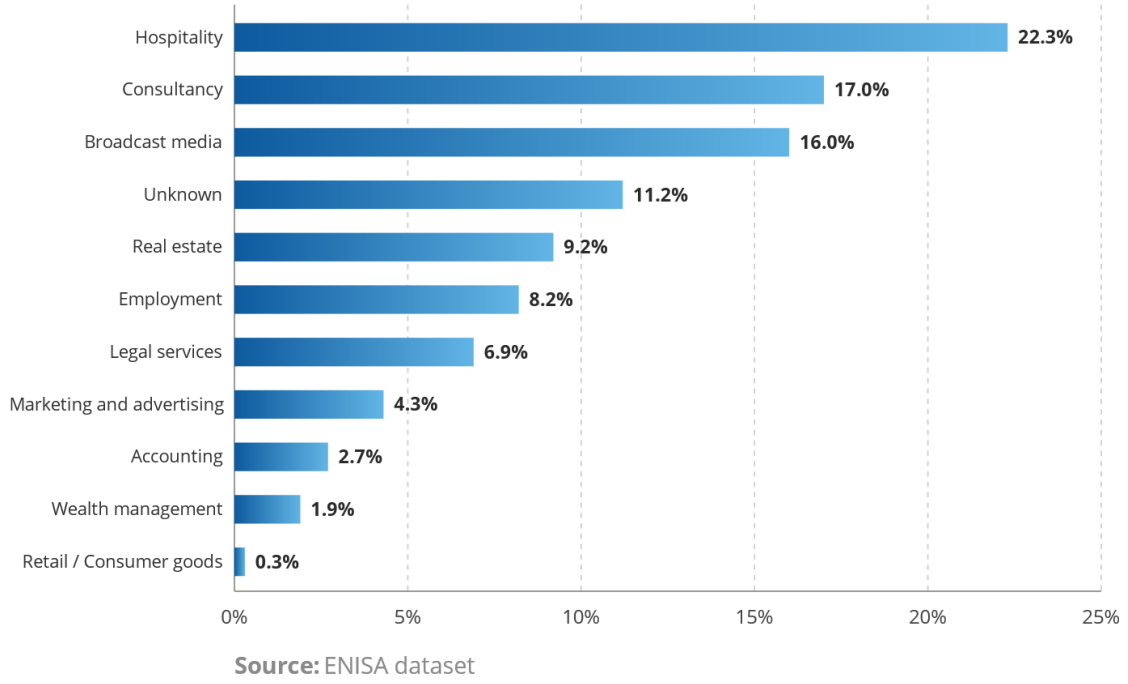


Figure 12 - Incidents impacting EU business services per subsector

Among all ideology-driven incidents impacting business services (47.3%), the highest number of claimed incidents originated from NoName057(16) (35.8%), followed by Mr Hamza (6.4%), Keymous+ (5.8%), Hezi Rash (4.2%) and TwoNet (3.9%). Z-Pentest Alliance and Akatsuki Cyber Team stood out for the number of their claimed intrusions affecting smaller commercial entities, such as media, marketing, hospitality and consultancy-related entities.

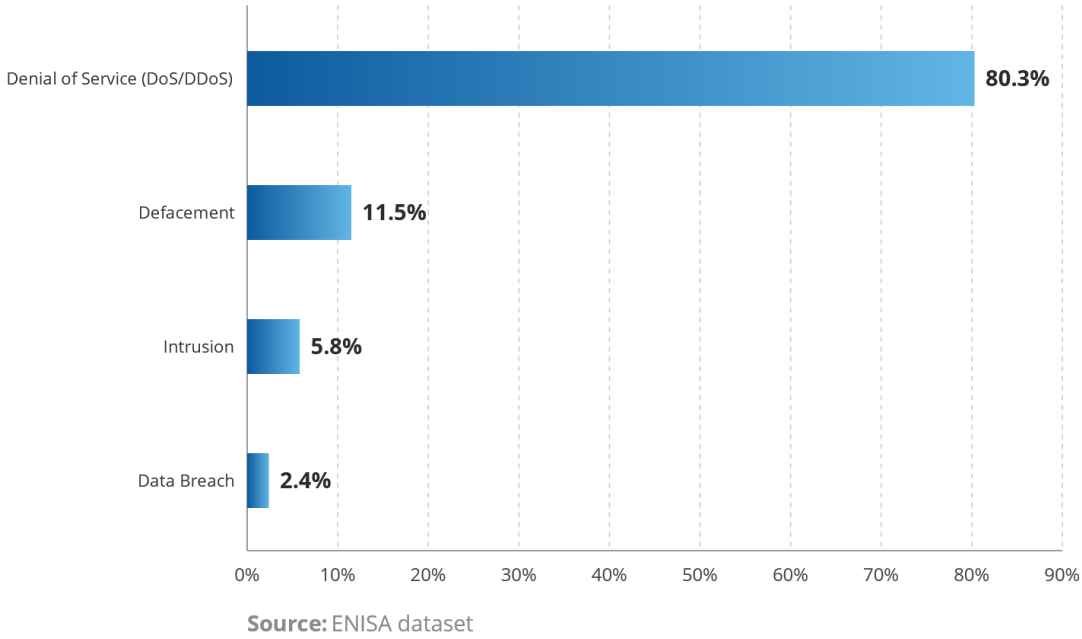


Figure 13 - Ideology driven incidents impacting business services in the EU

Within the financially motivated incidents targeting business services (46.8%), ransomware deployments represented most events (65.4%), followed by data breaches (28.4%). Most deployed ransomware strains against the sector include **Qilin (15.4%), SafePay (8.4%), and INC ransomware (6%)**.

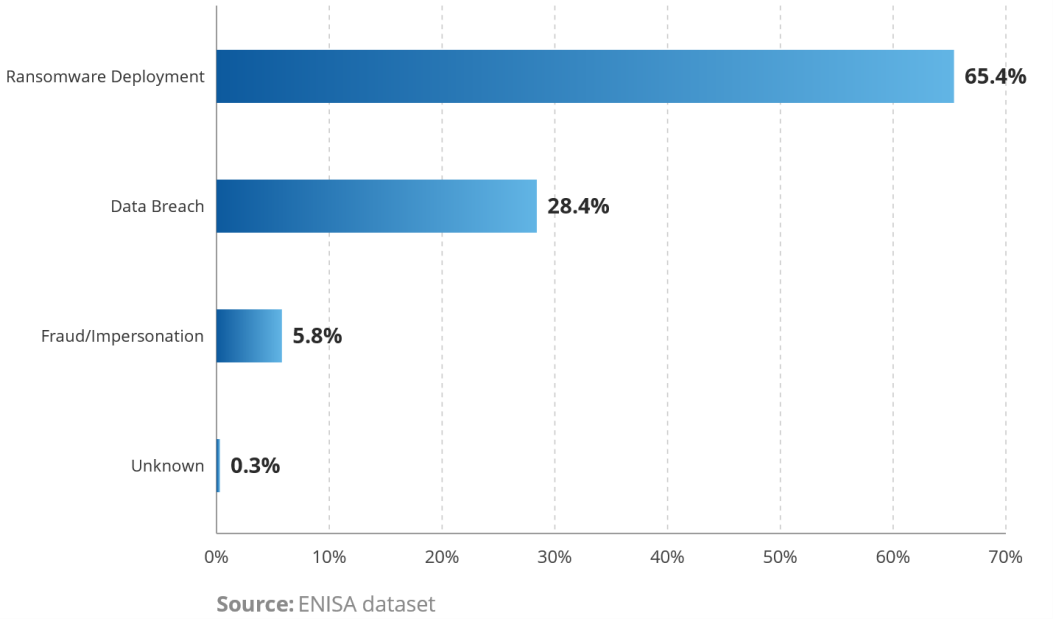


Figure 14 - Financially motivated incidents impacting business services in the EU

Business services were also impacted by the activities of State-nexus intrusion sets, mainly **through DPRK-nexus job-themed campaigns** targeting software developers and consultancy-related profiles. Famous Chollima (DPRK IT workers) and Lazarus were associated with activity involving fake or fraudulent IT-worker profiles, while Contagious Interview was linked to job-themed social-engineering campaigns using fake recruiter approaches and coding-test lures to deliver malware to freelance developers. Similar LinkedIn-based lures targeting developers in Czechia to steal credentials and cryptocurrency-wallet data, while reporting on Famous Chollima activity showed how developers operating under false identities attempted to infiltrate Western companies, including in France, to generate revenue for the North Korean state or enable follow-on extortion[96] [97] [98].

[96] https://www.welivesecurity.com/en/eset-research/deceptivedevelopment-targets-freelance-developers/
[97] https://dotekomanie.cz/2025/03/novy-druh-utoku-na-linkedinu-v-cesku-kyberzlocinci-lakaji-vyvojare-na-falesne-nabidky-prace-a-kradou-kryptomeny/
[98] https://www.lemonde.fr/pixels/article/2025/07/10/comment-la-coree-du-nord-infiltre-ses-experts-informatiques-au-c-ur-des-entreprisesoccidentales_6620374_4408996.html

2.3 Transport

The EU transport sector accounted for **8% of all events across sectors**. The sector also accounted for 8% of events with significant impact reported under the NIS2 Directive in 2025, placing it among the top five impacted sectors[99].Targeting was concentrated on **railway** (31.9%) and **air** (30.4%), followed by **road** (17.9%) and **water transport** (16.4%). A notable change compared with the previous ETL is the increased prominence of railway-related events, which once accounted for only 2% of events in the transport sector, as the second most affected transport subsector. This increase was mainly driven by repeated DDoS claims against operators of railways, metros and tramways services during H2 2025. Based on ENISA NIS360 report, railway and maritime transport are categorised as being in the risk zone, notably due to their reliance on heterogenous systems and their strategic importance in the global supply chain.

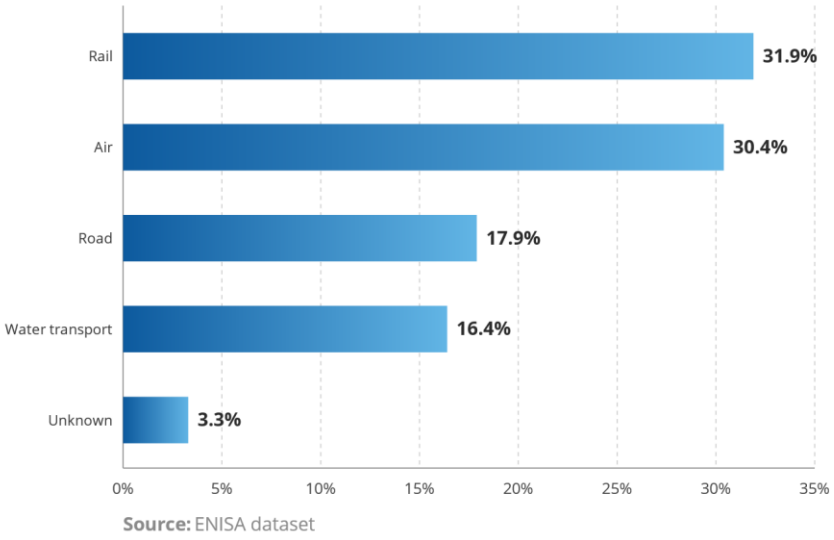


Figure 15 - Incidents impacting the EU transport sector per subsectors

The transport sector remained **largely impacted by DDoS claims (83.1%), followed by unauthorised access (16.3%).**

[99] https://ciras.enisa.europa.eu/ciras-consolidated-reporting

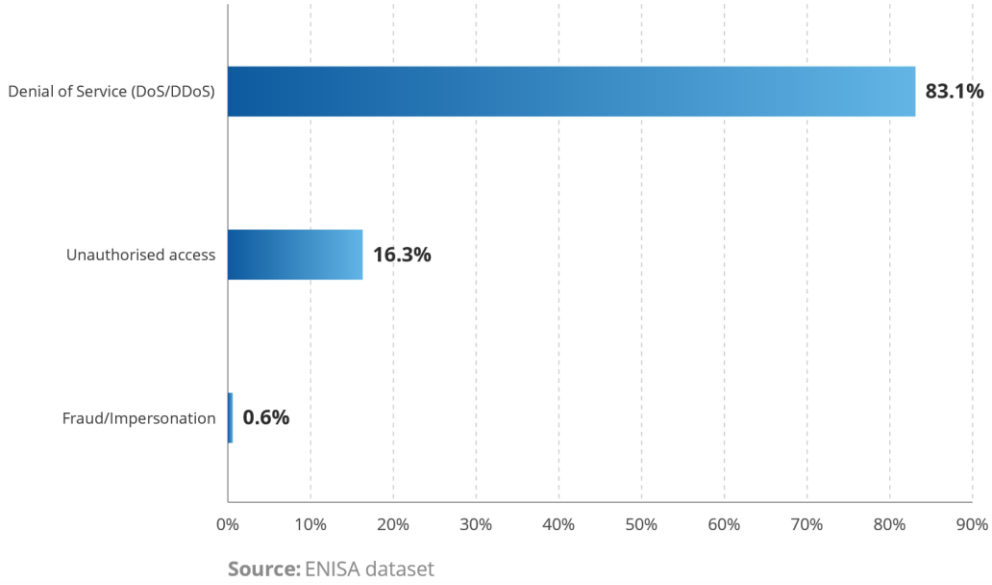


Figure 16 - Incident types impacting the EU transport sector

DDoS attacks conducted for ideology-driven purposes (98.6%) were notably linked to specific events at the EU national level and/or support for Ukraine. DDoS claims against this sector primarily originated from NoName057(16) (58%), Dark Storm Team (12.1%) and Server Killers (11.2%). In June 2025, around the time of the NATO Summit in The Hague, NoName057(16) claimed attacks against Dutch transport-related targets, including transport operators[100] [101] [102] [103] [104], as well as Schiphol, the Netherlands' main international airport and a key travel hub for summit-related transport. Of note, the European Union Aviation Safety Agency (EASA) reported on a 43.56% increase of hacktivist claims against European aviation websites, notably led by NoName057(16) and Dark Storm Team. In November 2025, NoName057(16) referred to Denmark's announcement of its 28th Ukraine-support package in its claims and/or threats against the Danish Ministry of Transport, DSB, public-transport portals, road-toll infrastructure and airport-related websites[105] [106] [107]. Several DDoS waves coincided with specific geopolitical developments, including the renewed German air-defence support discussions for Ukraine, Spain's November 2025 aid package for Ukraine, and the public condemnation of sabotage against a Polish railway line used for aid deliveries to Ukraine[108] [109] [110].

[100] hxxps://t.me/c/2634086323/99
[101] hxxps://t.me/c/2634086323/109
[102] https://nltimes.nl/2025/06/24/sabotage-may-behind-schiphol-rail-problems-cyberattack-hits-nato-summit-websites
[103] https://apnews.com/article/nato-summit-cybersecurity-hack-russia-netherlands-fa97bbf8797a51c2885d47f5f83691be
[104] https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/the-hague-summit-declaration
[105] hxxps://t.me/c/2787466017/296
[106] hxxps://t.me/c/2787466017/391
[107] https://cphpost.dk/2025-11-14/news/round-up/pro-russian-hackers-plan-to-attack-danish-websites/
[108] https://www.theguardian.com/world/live/2025/jul/17/ukraine-russia-war-patriot-nato-latest-europe-news-live-updates
[109] https://www.euractiv.com/news/spain-commits-e615-million-in-military-aid-to-ukraine/
[110] https://apnews.com/article/poland-sabotage-explosion-rail-track-warsaw-97dae3045d4e1ff329780526c6279c0f

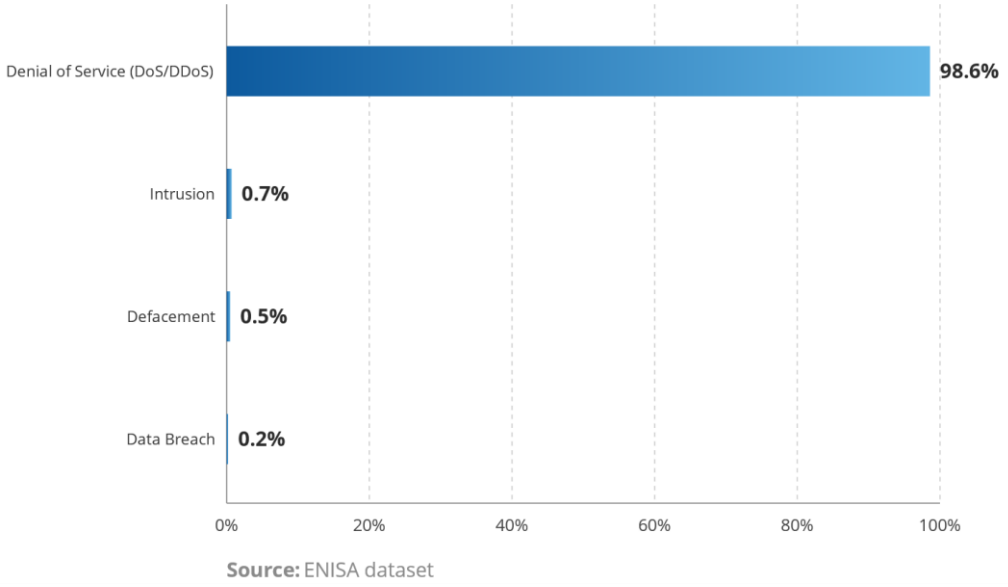


Figure 17 - Ideology driven incidents impacting the EU transport sector

Financially motivated incidents against the transport sector accounted for 10.2% of all attacks on that sector, with data breaches accounting for 56.7% and ransomware deployments for 37.3%. Data breaches incidents were notably driven by the exploitation of managed file-transfer software used in logistics and supply-chain environments, and data-theft campaigns affecting cloud, Customer Relationship Management (CRM), customer-service and third-party provider environments[111] [112]. Based on information shared by the European Union Aviation Safety Agency, the aviation sector saw at least 10 ransomware attacks in the EU in 2025, with Akira being the most deployed strain.

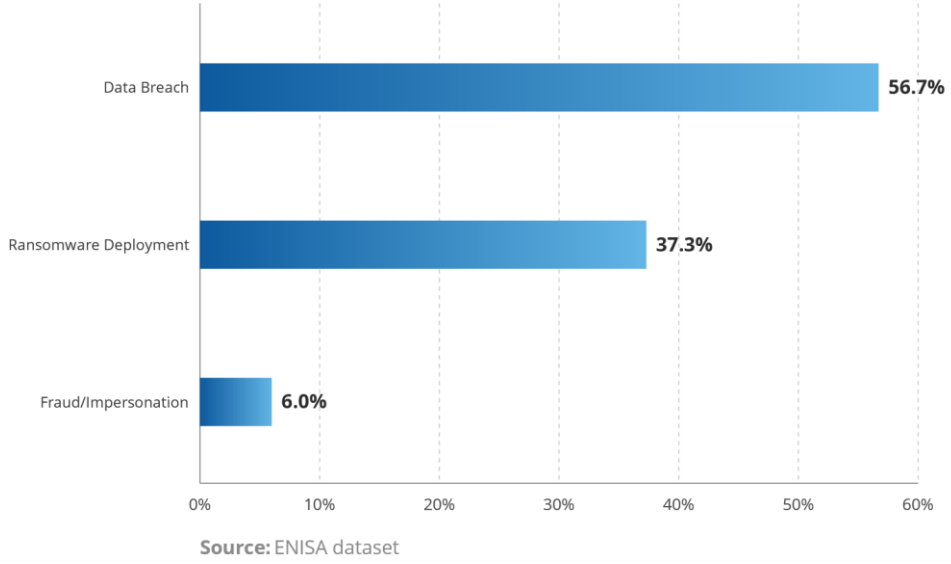


Figure 18 - Financially motivated incidents impacting the EU transport sector

[111] https://www.huntress.com/blog/threat-advisory-oh-no-cleo-cleo-software-actively-being-exploited-in-the-wild
[112] https://cloud.google.com/blog/topics/threat-intelligence/voice-phishing-data-extortion

Ransomware deployments against the transport sector notably include **Akira, Qilin, and Cl0p** (12% each) and resulted in disruptive impact in a few cases. The most significant case was the September 2025 ransomware incident affecting US-based Collins Aerospace's passenger-processing software, which disrupted automated check-in systems at several EU airports, including Brussels and Berlin, causing delays, cancellations and the use of manual check-in procedures[113] [114]. Two prominent examples of data breaches due to attacks against third-party provider environments were the confirmed unauthorised access to an external customer-service platform used by Air France-KLM, and the disclosure by Iberia of a third-party attack targeting one of their suppliers and affecting Iberia's customers[115] [116].

In 2025, the State-nexus activity recorded against the transport sector was largely linked to cyberespionage and strategic intelligence collection. **Maritime**-related organisations were primarily targeted by China-nexus **Mustang Panda**, with continuous campaigns impacting at least seven EU MSs. Iran-nexus group **Chafer** was also reported active against the sector, with a demonstrated interest in **air** transport related entities, with leaked material indicating the reconnaissance and targeting of global airlines, including European carriers[117].

Although logistics is treated separately from the transport sector for the purposes of this report, the two sectors remain operationally connected. Logistics entities support freight movement, warehousing, courier services and supply-chain continuity, and therefore share several exposure points observed in transport, including reliance on third-party platforms, managed file-transfer systems, customer and shipment data and public-facing service portals. **Logistics entities were primarily affected by cybercrime activity, with ransomware representing around half of the recorded incidents**, followed by DDoS claims, which accounted for approximately a quarter of the recorded incidents. Ransomware activity affected freight, warehousing, cold-chain, postal and courier, and third-party logistics providers, with Akira being the most frequently recorded ransomware group, followed by Cl0p, DragonForce and SafePay. DDoS activities were largely linked to NoName057(16) and targeted logistics and logistics-adjacent entities, including courier, freight and transport-service providers.

[113] https://www.dw.com/en/european-airports-disruption-due-to-ransomware-eu-agency/a-74073365
[114] https://www.reuters.com/en/cyberattack-causes-flight-delays-cancellations-brussels-airport-2025-09-20/
[115] https://nieuws.klm.com/klm-informeert-klanten-over-incident-met-persoonsgegevens/
[116] https://securityaffairs.com/184985/data-breach/iberia-discloses-security-incident-tied-to-supplier-breach.html
[117] https://blog.narimangharib.com/posts/2025%2F07%2F1752917718209?lang=en

2.4 Manufacturing

Manufacturing ranked fourth among the most targeted sectors, accounting for **6.9%** of all recorded events. The distribution of incidents affecting the sector over the reporting period shows a clear **focus on machinery and equipment (23.3%) and construction (21.8%)**.

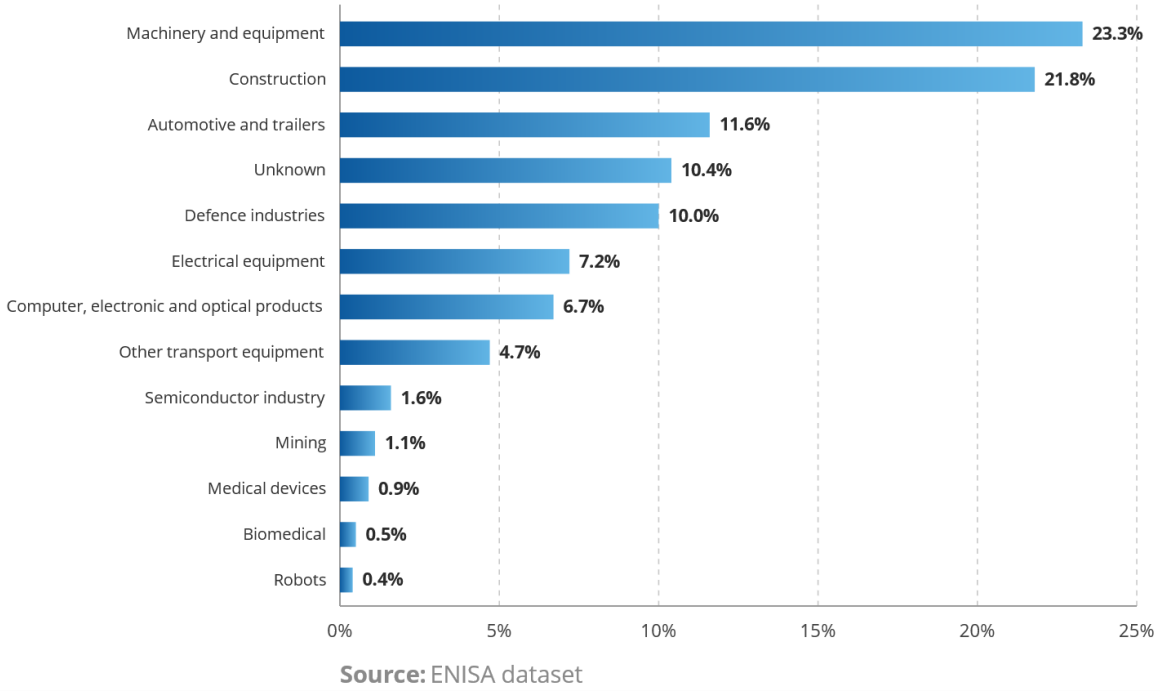


Figure 19 - Incidents impacting the EU manufacturing sector per subsectors

The manufacturing sector was primarily **impacted by unauthorised access (80.4%), followed by DDoS attacks (14.6%)**.

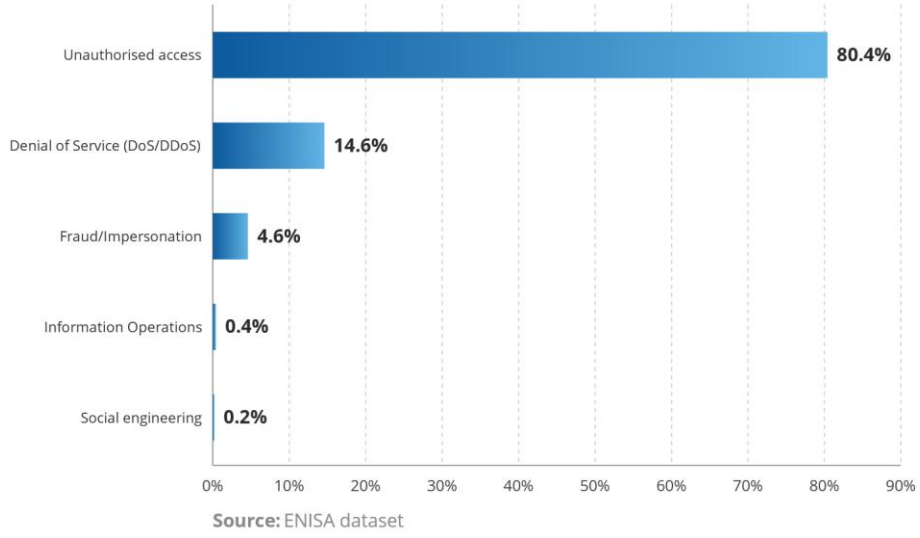


Figure 20 - Incident types impacting the EU manufacturing sector

Financially motivated incidents against the manufacturing sector accounted for 61.1% of all incidents targeting this sector, with ransomware deployments accounting for 82.8%, followed by data breaches (14.1%). Among ransomware deployments, the most deployed ransomware strains include **Qilin (17.4%), Akira (11.5%) and SafePay (8%).** Ransomware was particularly prevalent among machinery and equipment, construction, automotive, electronics and electrical-equipment manufacturers. In terms of impact, publicly reported cases show that incidents continued to affect core IT systems, the most notable resulting in service degradation and operational disruption[118] [119], with a few identified cases **impacting cross-site operations**. For instance, an incident impacting a German heat-exchanger manufacturer reportedly disrupted its subsidiaries in Poland and China[120] [121] [122]. Another example is a ransomware incident that targeted Japan-based Okuma Corporation and affected its German subsidiary, Okuma Europe GmbH[123].

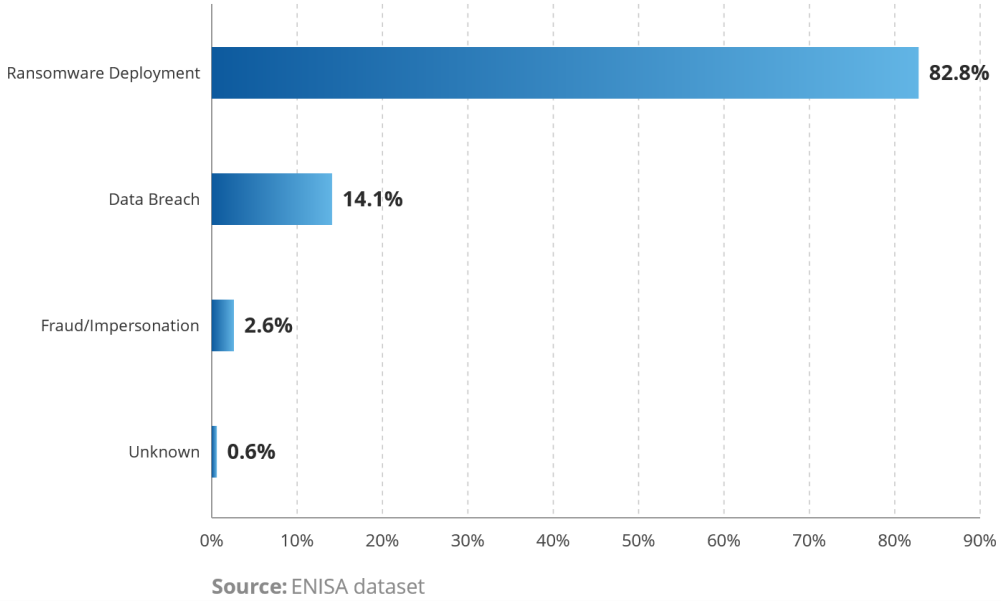


Figure 21 - Financially motivated targeting the EU manufacturing sector

Ideology-driven incidents (24.2%) against the manufacturing sector primarily involved DDoS (60.1%), followed by intrusion and defacements claims (24.6% and 10.1% respectively).

Similarly to the targeting of previously documented sectors, **hacktivist activities against this sector were primarily grounded in the context of the support for Ukraine from EU MSs. DDoS claims were** led by NoName057(16) (51.8%)[124] [125], as illustrated by claims between March and April 2025 against manufacturing, aerospace and defence, and construction related websites after Belgium

[118] https://www.baer-cargolift.com/en_GB/cyber
[119] https://www.bar-cargolift.dk/blog/nyt-6/gerd-bar-gmbh-is-fully-operational-again-after-cyber-attack-as-of-17-february-2026-320
[120] https://ics-cert.kaspersky.com/publications/a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity-q3-2025/
[121] https://www.all-about-security.de/cyberangriff-auf-thermofin-gmbh-personenbezogene-daten-betroffen/
[122] https://www.freiepresse.de/vogtland/reichenbach/vogtlaendisches-unternehmen-opfer-von-cyberangriff-wir-kaempfen-um-die-produktion-am-laufen-zu-halten-artikel13970410
[123] https://www.okuma.co.jp/english/news/2025/250925.php
[124] https://cybernews.com/security/noname-launch-ddos-attacks-in-germany/
[125] https://www.link11.com/en/blog/threat-landscape/camouflage-deception-overload-layer-7-ddos-attack-in-the-shadow-of-the-noname05716-attacks/

announced EUR 1 billion military aid package for Ukraine[126]. The higher volume of unverified intrusion claims against the sector notably pertained to the **increased targeting of operational technology (OT)**[127] [128].

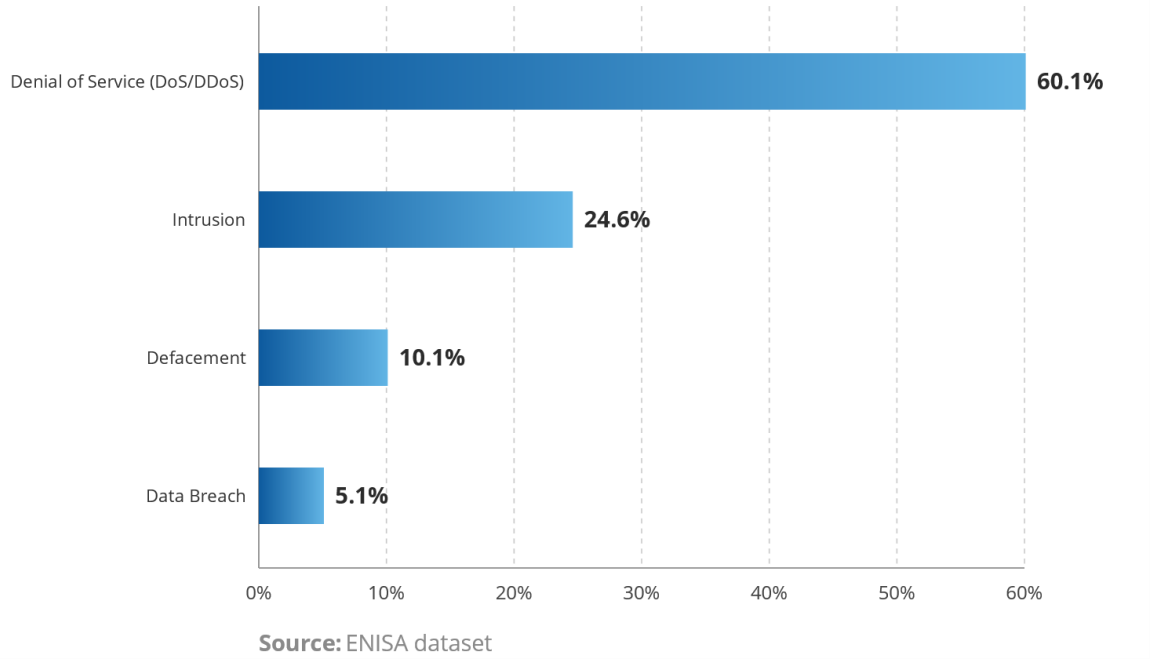


Figure 22 - Ideology motivated targeting the EU manufacturing sector

Reports mentioning **the targeting of the manufacturing sector by State-nexus intrusion sets in the EU** (8.4%) primarily pertained to the targeting of **defence-related organisations**, as illustrated by campaigns associated to DPRK-nexus Lazarus, Russia-nexus DragonFly and Storm-2372 and Iran-nexus Nimbus Manticore[129] [130] [131] [132]. Another large-scale campaign aligned with China-nexus interests involving PurpleHaze and ShadowPad ran from July 2024 to March 2025 and impacted over 70 global targets, including multiple entities in manufacturing[133]. **It is plausible that part of these activities pertained to the theft of intellectual property.**

[126] https://ccb.belgium.be/open-media/1218/download?inline
[127] https://www.group-ib.com/resources/research-hub/europe-manufacturing-threat-report/
[128] https://media.defense.gov/2025/Dec/09/2003840175/-1/-1/0/JOINT_CSA_PRO-RUSSIA_HACKTIVISTS_CONDUCT_ATTACKS_AGAINST_CRITICAL_INFRASTRUCTURE.PDF
[129] https://www.welivesecurity.com/en/eset-research/gotta-fly-lazarus-targets-uav-sector/
[130] https://blog.talosintelligence.com/static-tundra/
[131] https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/
[132] https://ics-cert.kaspersky.com/publications/reports/2025/12/01/apt-and-financial-attacks-on-industrial-organizations-in-q3-2025/
[133] https://www.sentinelone.com/labs/follow-the-smoke-china-nexus-threat-actors-hammer-at-the-doors-of-top-tier-targets/

2.5 Finance / Banking

The finance / banking sector accounted for 5.6% of all events collected primarily impacted by unauthorised access (46%) and DDoS attacks (38.9%), followed by fraud and impersonation (14.8%). Of note, EU MSs reported that 10% of incidents with a significant impact in 2025 impacted the banking sector[134].

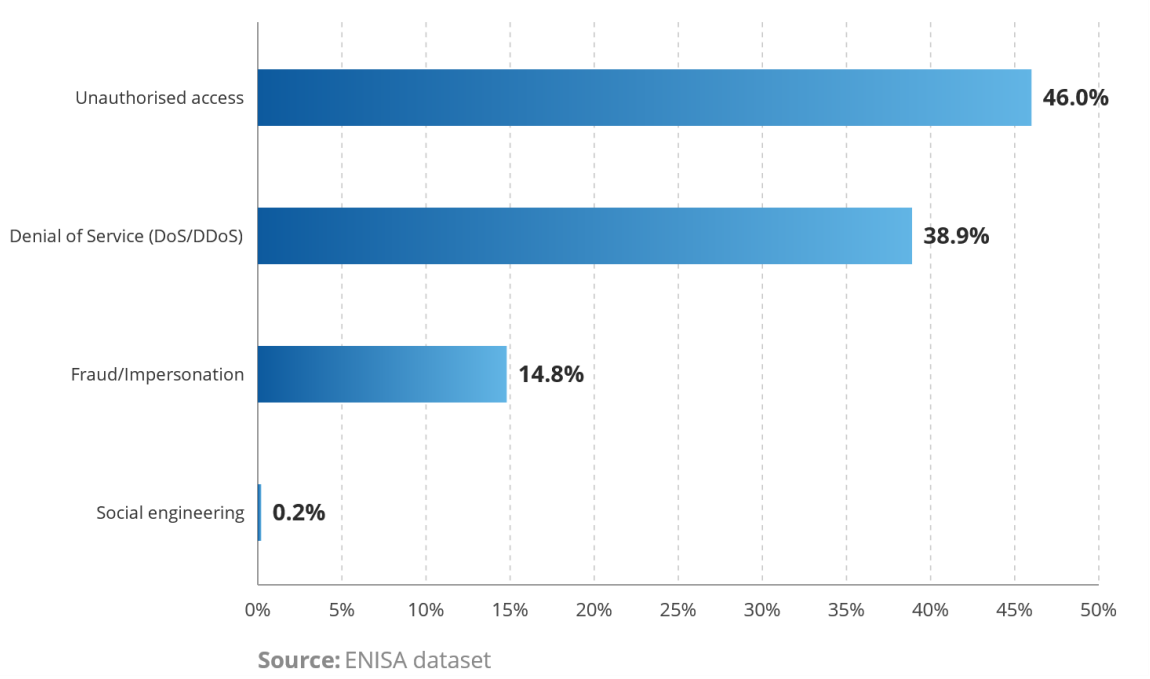


Figure 23 – Incident types impacting the EU finance/ banking sector

As they process a significant amount of valuable data, **financial institutions represent high value targets for cybercriminals**; financially motivated incidents primarily involved unauthorised access (81.6%) followed by fraud/impersonation (17.9%). Data breaches were particularly relevant in the insurance, banking and credit-institutions subsectors. In the insurance subsector, reported cases included the cyberattack affecting Generali Tranquilidade, where the personal data of customers was reportedly exposed, and the data breach that impacted former customers of Liberty and BBVA Seguros through Generali España[135] [136]. Ransomware deployments against the finance sectors notably included **Akira (20%), Lynx, Qilin and INC Ransom** (8% each).

[134] https://ciras.enisa.europa.eu/ciras-public
[135] https://www.publico.pt/2025/06/24/tecnologia/noticia/dados-clientes-generali-tranquilidade-comprometidos-ciberataque-2137713
[136] https://www.eleconomista.es/banca-finanzas/noticias/13250519/03/25/generali-sufre-un-ciberataque-que-afecta-a-los-ex-clientes-de-liberty-y-de-bbva-seguros.html

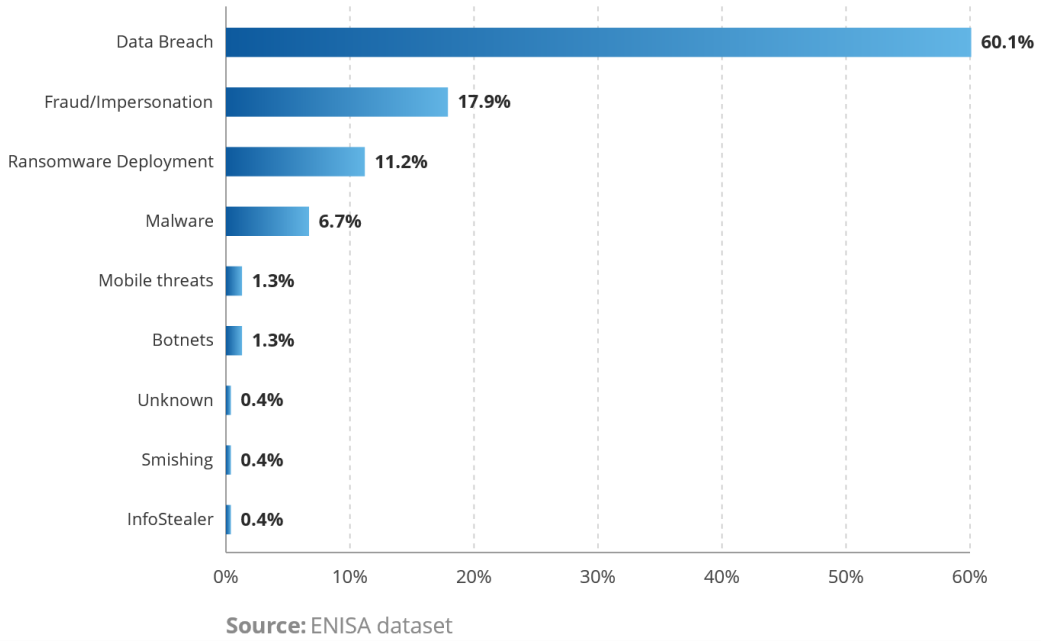


Figure 24 - Financially motivated incidents impacting the EU finance/ banking sector

The distribution of incidents affecting finance / banking shows a **clear concentration in credit institutions (61.9%)**, followed by insurance with 17.8%, while crypto-asset service providers represented 7.7%.

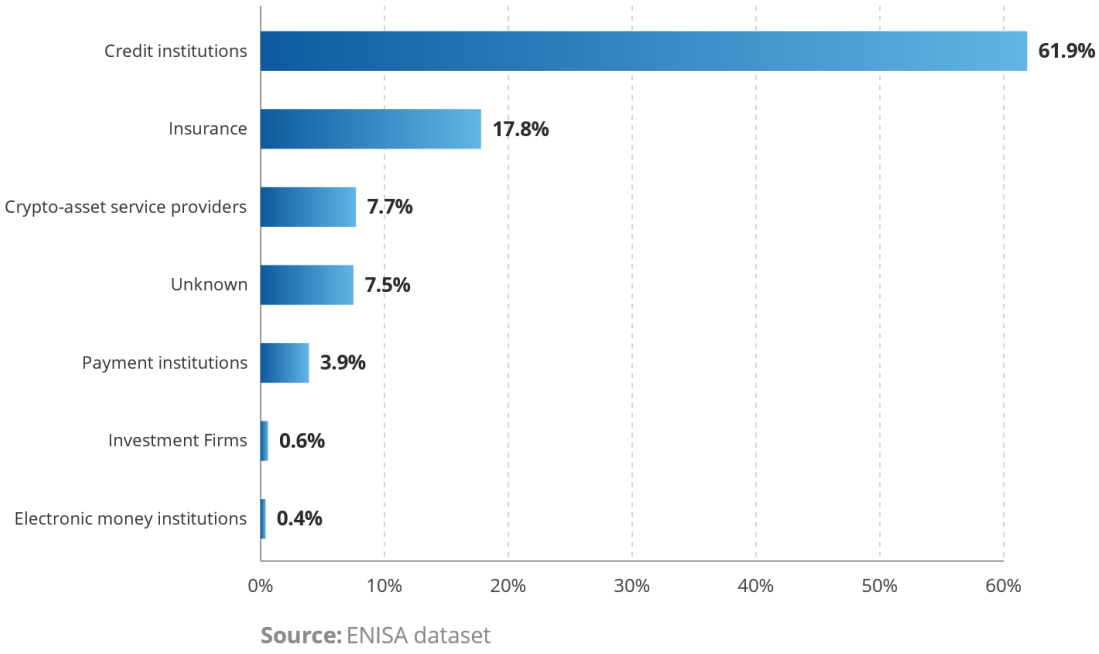


Figure 25 - Incidents impacting the EU finance / banking sector per subsectors

Ideology-driven attacks represented 40.6% of incidents targeting the finance/banking sector, with a prevalence of DDoS claims (95.8%) followed by defacements (2.1%) and intrusion claims (1.6%). Ideology-driven DDoS attacks against the finance/banking sector were primarily claimed by **NoName057(16) with 40.7%, followed by Keymous+ (9.5%) and Dark Storm Team (8.5%)**. DDoS claims identified by ENISA indicated a particular focus on public-facing banking and insurance portals[137]. It is highly likely finance/banking would represent a valuable target for hacktivist groups as a temporary interruption of website availability would impact several thousand customers and would also be reported by mainstream media, creating a second layer of disruption to business continuity, in addition to reputational damage. As was often the case throughout the reporting period, these claims were part of multi-sector hacktivist campaigns as illustrated in NoName057(16)'s targeting of Germany in April 2025, that notably involved the targeting of finance/banking alongside municipalities, manufacturers and other companies, in a campaign framed around geopolitical developments and support for Ukraine[138] [139].

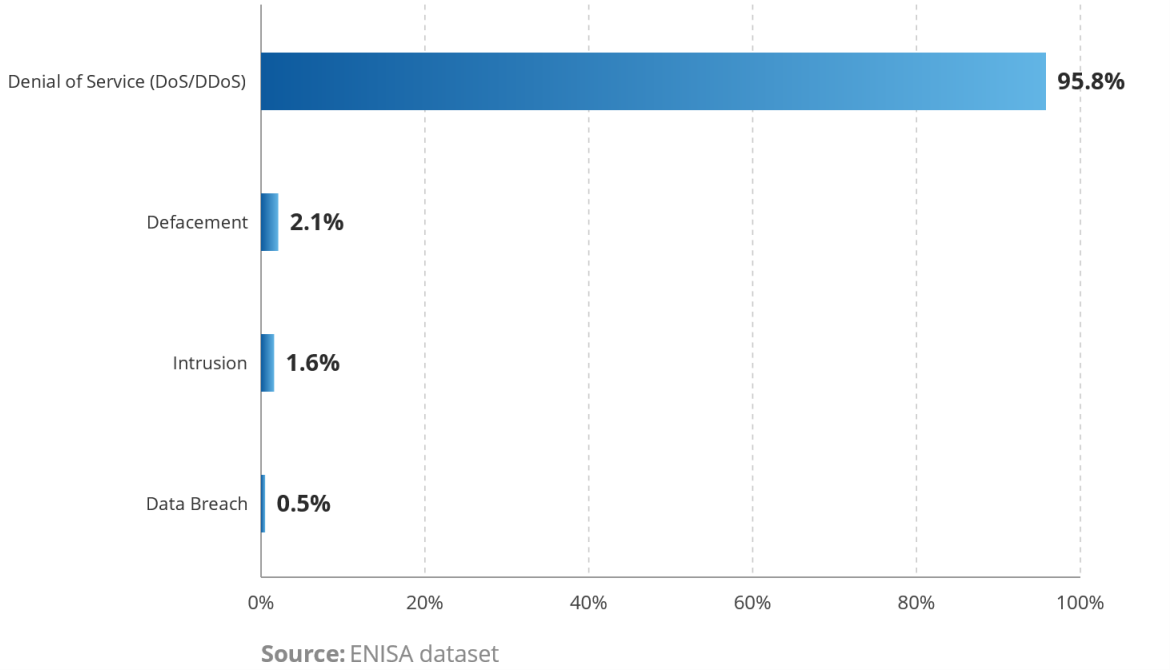


Figure 26 - Ideology motivated incidents impacting the EU finance/ banking sector

Based on reports mentioning the targeting of the finance/banking sector by **State-nexus activities in the EU (2.8%), activities that were recorded primarily pertained to crypto-asset service providers and high-value financial-sector personnel**. DPRK-nexus activity, including campaigns associated with BlueNoroff and Famous Chollima, targeted cryptocurrency foundations, developers and IT professionals, likely in support of financially motivated operations and cryptocurrency theft[140] [141] [142]. Separately, Graphite spyware was reportedly used against a high-profile banking executive,

[137] https://www.americanbanker.com/news/pro-russia-hackers-target-italian-banks-with-ddos-attack
[138] https://cybernews.com/security/noname-launch-ddos-attacks-in-germany/
[139] https://www.link11.com/en/blog/threat-landscape/camouflage-deception-overload-layer-7-ddos-attack-in-the-shadow-of-the-noname05716-attacks/
[140] https://securelist.com/bluenoroff-apt-campaigns-ghostcall-and-ghosthire/117842/
[141] https://www.huntress.com/blog/inside-bluenoroff-web3-intrusion-analysis
[142] https://www.trendmicro.com/en_gb/research/25/d/russian-infrastructure-north-korean-cybercrime.html

indicating that **senior financial-sector personnel may also represent targets of interest for surveillance activity**[143].

HEALTH & DIGITAL INFRASTRUCTURE

As previously mentioned, the health and digital infrastructure sectors appeared in the top five of impacted sectors according to EU MSs NIS2 reporting. Given their critical role in the provision of essential services and the potential impact of cyber incidents on their operations and dependent sectors, selected highlights from ENISA's OSINT monitoring are presented below.

The health sector threat picture was primarily shaped by unauthorised access, led by financially motivated attacks (46%). Out of these, ransomware deployments accounted for 26.8%; the most deployed ransomware strains include Qilin, INC ransom and SafePay. Ransomware continued to have direct operational consequences for healthcare delivery, as illustrated by the Stell Hospital and the Gers Hospital Centre cases[144] [145] [146]. Data breaches were mainly recorded against healthcare providers (63.6%) as seen for the Hôpital Privé de la Loire[147]. DDoS attacks primarily targeted healthcare providers, which observed 85.5% of DDoS claims, with the most active groups including Hezi Rash, Dark Storm Team, and Keymous+. In 2025, ENISA published a cyber hygiene guide for the health sector, providing practical steps to strengthen the sector's resilience[148].

Digital infrastructure was primarily targeted by DDoS (50.6%), followed by unauthorised access (40.4%) for financially motivated (20.3%) and cyberespionage (10.5%) purposes. 70.9% of financially motivated unauthorised accesses involved data breaches, followed by ransomware deployments (25.3%), with Qilin, Kraken, Lynx, Babuk2, Akira and Hunters International being the most deployed strains. Providers of publicly available electronic communications services was the most targeted subsector (53.5%), with the highest count of DDoS attacks (32.1%), notably carried out by NoName057(16) and Keymous+.

[143] https://irpimedia.irpi.eu/sorveglianze-paragon-colpisce-ancora-anche-lad-di-unicredit-tra-i-bersagli/
[144] https://www.zataz.com/apres-la-cyberattaque-lhopital-stell-sorganise-et-resiste/
[145] https://cyberveille.esante.gouv.fr/retours-d-experience/compromission-du-si-et-ransomware-au-chd-stell-2025-10-14
[146] https://www.ladepeche.fr/2025/08/07/le-centre-hospitalier-du-gers-cible-par-une-cyberattaque-une-enquete-est-en-cours-12865493.php
[147] https://www.leprogres.fr/faits-divers-justice/2025/07/10/piratage-informatique-au-hpl-que-risquent-les-patients-qui-se-sont-fait-voler-leurs-donnees
[148] https://www.enisa.europa.eu/sites/default/files/2025-09/ENISA%20Cyber%20Hygiene%20in%20the%20Health%20Sector.pdf

3. Cybercrime Threats

Cybercrime remained a main threat across the EU during the reporting period, representing 29.3% of the total number of events identified, resulting in the disruption of business continuity in several instances and ultimately resulting in financial loss to the Single Market. In 2025, the European Banking Authority reported that online investment fraud alone reportedly cost an estimated €4.2 billion across the European Economic Area (EEA) in 2024[149].

This section focuses on financially motivated activities including data breaches, ransomware claims and fraud schemes. Data breaches continued to affect organisations across multiple sectors, exposing personal, financial and corporate information that could be further exploited in malicious cyber operations. Ransomware deployments continued disrupting operations, notably through data encryption. Fraud schemes, including business email compromises, payment diversions, scams and investment fraud, also remained widespread.

In 2025, ransomware (47.3%) and data breaches (36%) formed most of the recorded financially motivated claims, followed by fraud and Impersonation (13.3%).

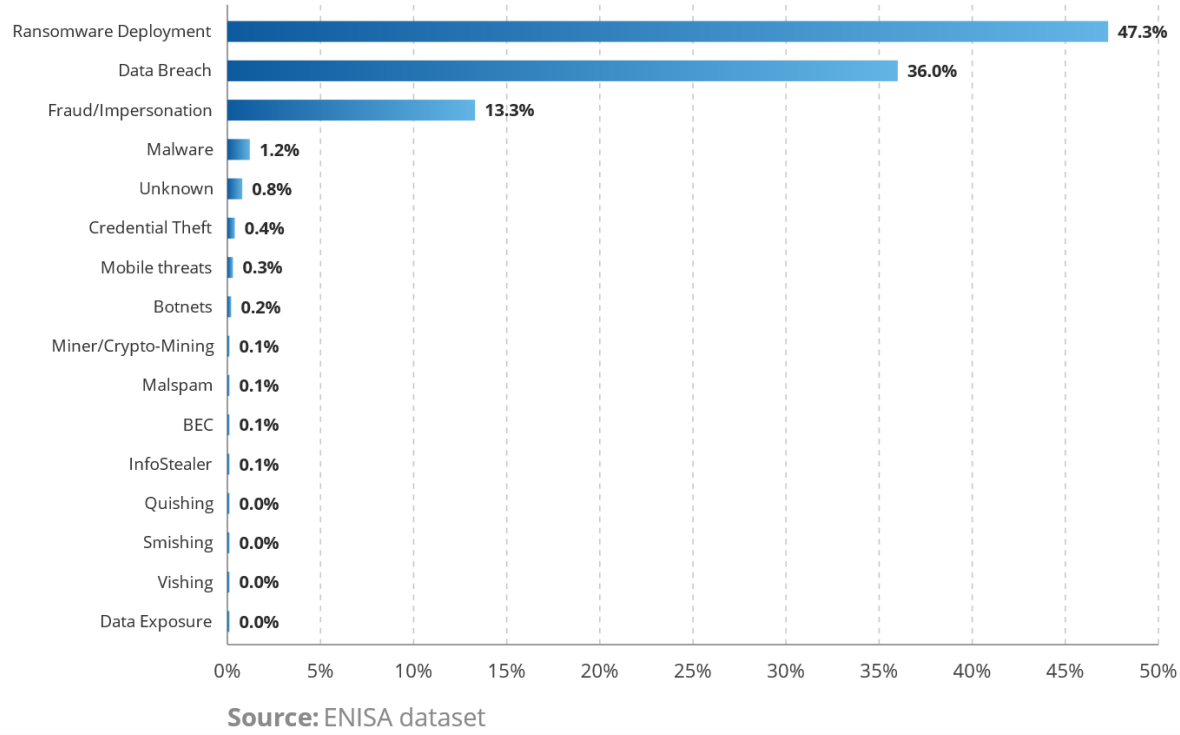


Figure 27 - Financially motivated incident types targeting the EU

[149] https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202512.en.pdf

3.1 Key threats

The next three sections provide details about the main type of events related to cybercrime and analysed by ENISA, namely fraud and impersonation, data breaches and ransomware.

3.1.1 Fraud and Impersonation

This section focuses on fraud and impersonation schemes impacting the EU. Fraud and scams are deceptive practices for financial purposes. ENISA's collection stems from sources such as underground forums and open-source reporting. In addition, ENISA also collected information pertaining to phishing campaigns involving impersonation attempts, notably through warnings issued by national cyber authorities.

The data collected data shows that out of the known groups seen conducting fraud and impersonation in the EU (24.4%), **Smishing Triad, mydocs and Hazy Hawk were identified as the most active.**

Active since at least 2024, China-based Smishing Triad notably conducted large-scale smishing campaigns targeting logistics providers and public administration services, using automated infrastructure to distribute messages and monetise stolen data, especially in Germany[150] [151].

Mydocs, an operator that emerged during a campaign against luxury hotels in Italy, appears to facilitate fraud and impersonation-related activity through underground forums where it advertises data such as personally identifiable information (PII)[152]. Such data is commonly used to support phishing, identity fraud and social engineering operations.

Hazy Hawk, active since at least December 2023[153], hijacked cloud resources and abandoned subdomains belonging to government agencies, universities and private organisations to host malicious URLs linked to scams and malware delivery. In February 2025, the operator was notably observed conducting impersonation-related activity targeting high-profile organisations in France, Sweden and Czechia since at least December 2023[154].

[150] https://unit42.paloaltonetworks.com/global-smishing-campaign/
[151] https://www.silentpush.com/blog/smishing-triad/
[152] https://www.acn.gov.it/portale/documents/20119/923891/operational_summary_ago2025_CLEAR_EN.pdf
[153] https://cybersecuritynews.com/hazy-hawk-exploits-organizations/
[154] https://www.infoblox.com/blog/threat-intelligence/cloudy-with-a-chance-of-hijacking-forgotten-dns-records-enable-scam-actor/

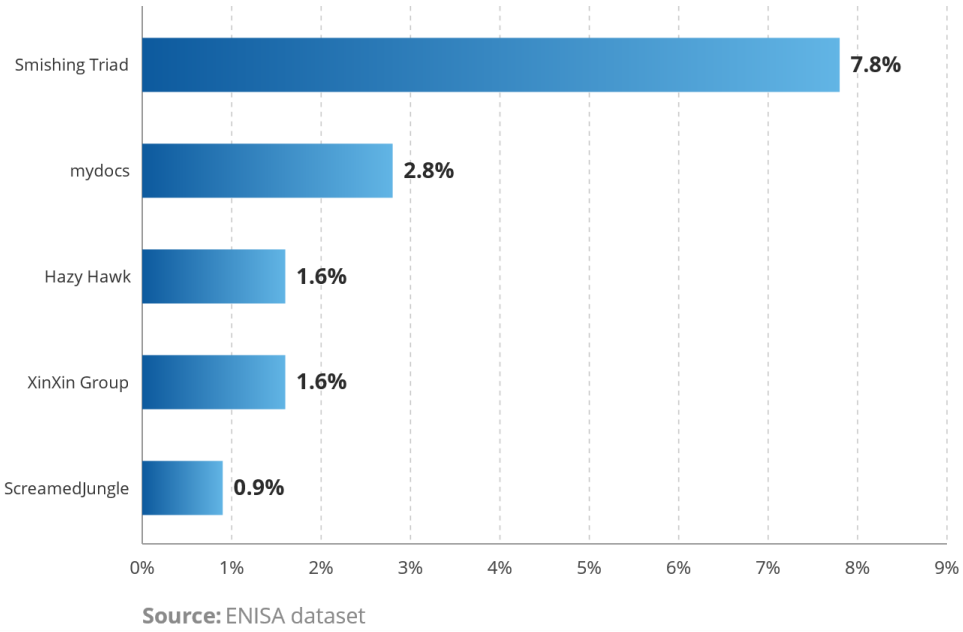


Figure 2928 - Top 5 groups claiming frauds impacting the EU

Email-based phishing methods formed the majority of phishing activity during the reporting period. Other publicly reported activity included SMS-phishing (smishing), voice phishing (vishing) and Quick Response (QR) code phishing (quishing). Additional techniques included ClickFix[155], malvertising, Business Email Compromise (BEC), malspam and FileFix[156]. Public reporting also highlighted a range of phishing campaigns masquerading as trusted brands, government and legitimate software to increase credibility. In regard to the popularisation of the PhaaS framework, XinXin Group (aka Black Technology), the developer of the Lucid PhaaS, has been active since 2023. While initially operating at a local level, its geographical reach has expanded[157].

Fraud and impersonation-related activity in 2025 was particularly identified in Italy (7.5%), followed by Spain with 6.3% and France with 4.7%. Of note, fraud and impersonation was primarily documented at a regional level in open sources, with Europe (including the EU) accounting for 24.7%.

[155] ClickFix is a social engineering technique that tricks users into executing malicious PowerShell commands which are automatically copied to their clipboard
[156] ClickFix variant
[157] https://catalyst.prodaft.com/public/report/lucid/overview

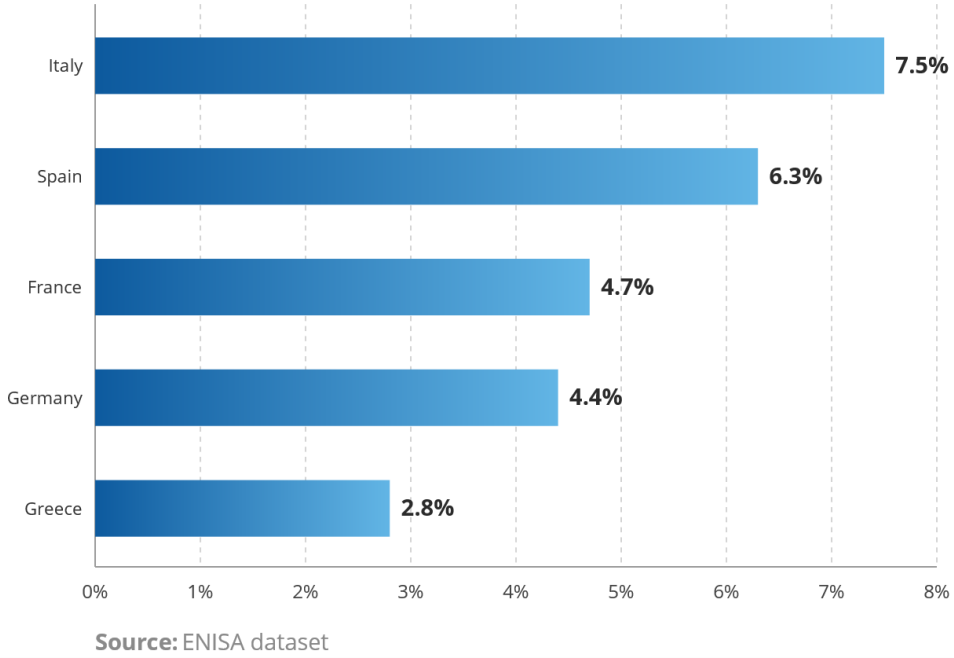


Figure 290 - Fraud schemes impacting EU MSs

Smishing Triad notably targeted France, Ireland, Poland, Germany and Lithuania, whereas Hazy Hawk focused on Italy, France, Czechia and Sweden. The collected data further indicates that **Italy and France were targeted by multiple intrusion sets during the reporting period**.

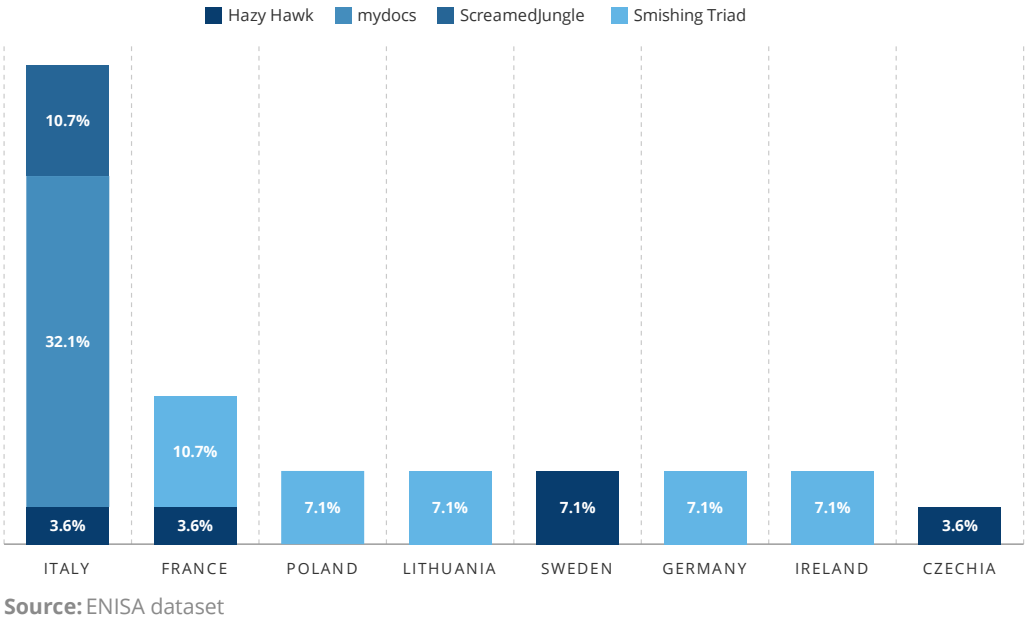


Figure 31 - Top 5 intrusion sets involved in fraud in the EU

Fraud and impersonation-related activity during the reporting period primarily affected digital providers with 16.6%, followed by public administration with 13.4%, and finance/banking (12.5%). Civil Society accounted for 9.4%, followed by business services (5.9%). The observed distribution

indicates that fraud schemes mainly targeted sectors involved in financial transactions, digital services and the handling of high value data such as financial and personal information. The concentration of activity affecting banking institutions and citizen-facing services highlights the continued use of financially motivated fraud and social engineering operations during the reporting period.

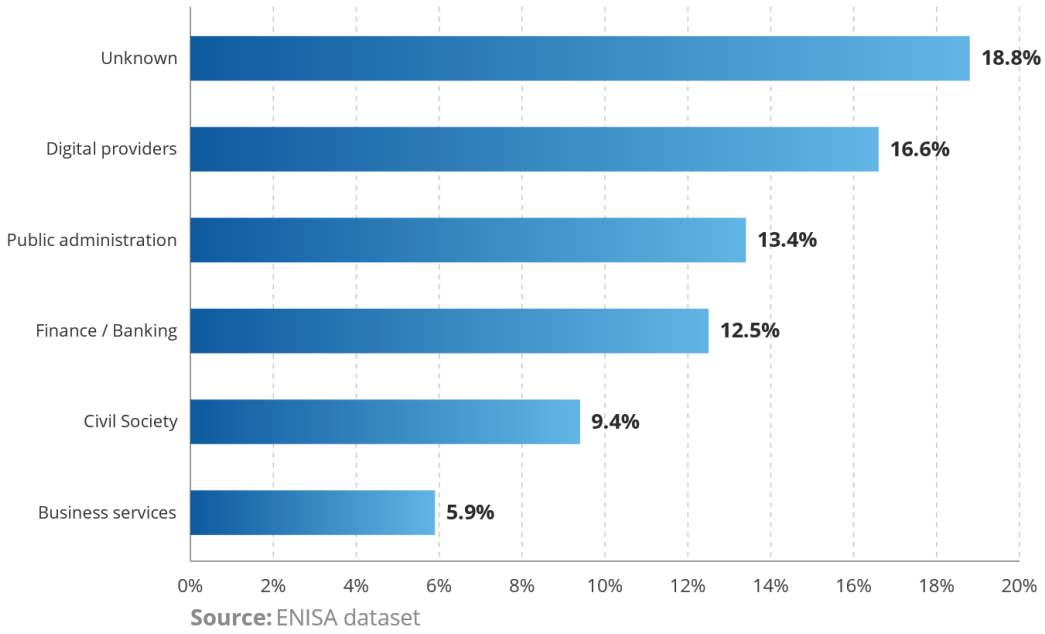


Figure 32 - Top 5 Sectors impacted by fraud and impersonation in the EU

Fraud and scam related incidents were notably carried out through websites designed to attract and deceive individuals by promising easy profits and appearing as legitimate, known as Baiting News Sites (BNS) thus contributing to enabling fraud[158] [159]. The use of AI further facilitates and increases the tempo of these activities, as they allow for better customisation of deceitful content[160] [161].

3.1.2 Data breaches

Data breaches remained a concern, exposing personal, financial and corporate information to be used for further malicious cyber activities. This section focuses on data breaches claims advertised for sale on cybercriminal forums; the authenticity or currency of these claims could not be verified.

[158] https://blog.knowbe4.com/thousands-of-spoofed-news-sites-push-investment-scams
[159] https://www.ctm360.com/reports/baittrap-rise-of-baiting-news-sites
[160] https://www.eba.europa.eu/sites/default/files/2025-12/fa63af9a-bafd-4821-baee-48c7c8fb6490/AI%20and%20online%20financial%20fraud%20and%20scams%20factsheet.pdf
[161] https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/777940/EPRS_ATA(2025)777940_EN.pdf

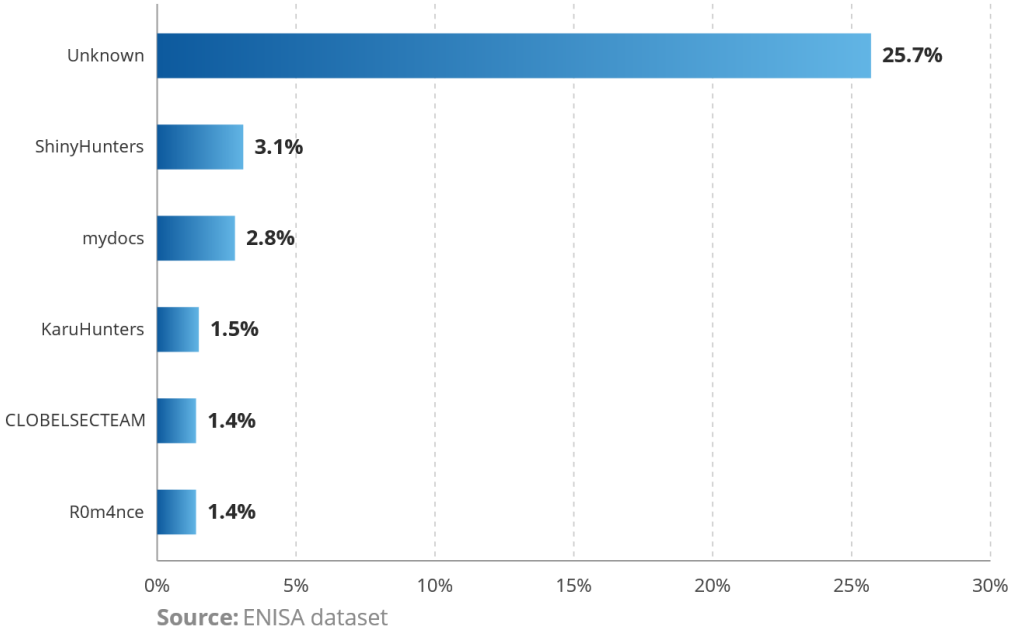


Figure 33 - Top 5 groups claiming data breaches in the EU

Out of the collected events categorised as data breaches and associated to a specific operator, ShinyHunters and mydocs accounted for the highest share of observed activity with 3.1% and 2.8% respectively[162] [163], followed by KaruHunters (1.5%), CLOBELSECTEAM and R0m4nce each representing 1.4%. This distribution illustrates the heterogeneity of the data breach and IAB ecosystems.

Data breach activity in 2025 continued to involve the exploitation of third-party platforms, sales of unauthorised access and the targeting of public services. A major trend involved the compromise of shared platforms and service providers affecting multiple organisations. The activities observed included attacks affecting Software-as-a-Service (SaaS) and CRM environments, third-party providers and developer infrastructure[164] [165] [166]. Intrusion sets also continued to advertise credentials, VPN and RDP access, database access and compromised backend environments on underground forums[167] [168] [169].

Large-scale theft of identity and financial data remained common during the reporting period. Identified examples included underground forums claiming the sale of Spanish citizen databases and identity records[170]. Additional listings advertised the sale of financial data such as IBAN information from various banks across the EU[171].

[162] https://www.bleepingcomputer.com/news/security/shinyhunters-behind-salesforce-data-theft-attacks-at-qantas-allianz-life-and-lvmh/
[163] https://www.techzine.eu/news/security/133612/airfrnace-klm-reports-data-breach-at-customer-service/
[164] https://cybernews.com/cybercrime/samsung-germany-customer-data-breach/
[165] https://www.infostealers.com/article/samsung-tickets-data-leak-infostealers-strike-again-in-massive-free-dump/
[166] https://www.trellix.com/en-in/blogs/research/amadey-exploiting-self-hosted-gitlab-to-distribute-stealc/
[167] https://doublepulsar.com/2022-zero-day-was-used-to-raid-fortigate-firewall-configs-somebody-just-released-them-a7a74e0b0c7f
[168] hxxps://forum.exploit.in/topic/260988/
[169] https://cloudprotection.com/blog/salesforce-attacks-in-2025/
[170] https://dailydarkweb.net/dark-web-post-alleges-sale-of-spanish-bank-and-crypto-accounts/
[171] hxxps://darkforums.st/Thread-Selling-IBAN-LEADS-Germany-France-Spain-Italy19622

Source code breaches were primarily observed on underground forums advertising stolen proprietary application code and compromised development repositories[172] [173]. Examples of such observed activity included references to confirmed breaches affecting Europcar, RedHat and ENEA [174] [175] [176] [177] [178] [179] [180].

Data breach claims were primarily related to organisations based in Spain, France, Italy, Germany and the Netherlands, which accounted for the highest volume of observed activity, with incidents linked to multiple groups, particularly ShinyHunters, Lapsus$, R0m4nce and CLOBELSECTEAM. In France, data breaches were primarily claimed by ShinyHunters, as well as Lapsus$ and breach3d. Claims relevant to organisations in Spain originated from operators that included Perro, BreachParty, and paysiano [181] [182] [183] [184] [185] [186] [187] [188].

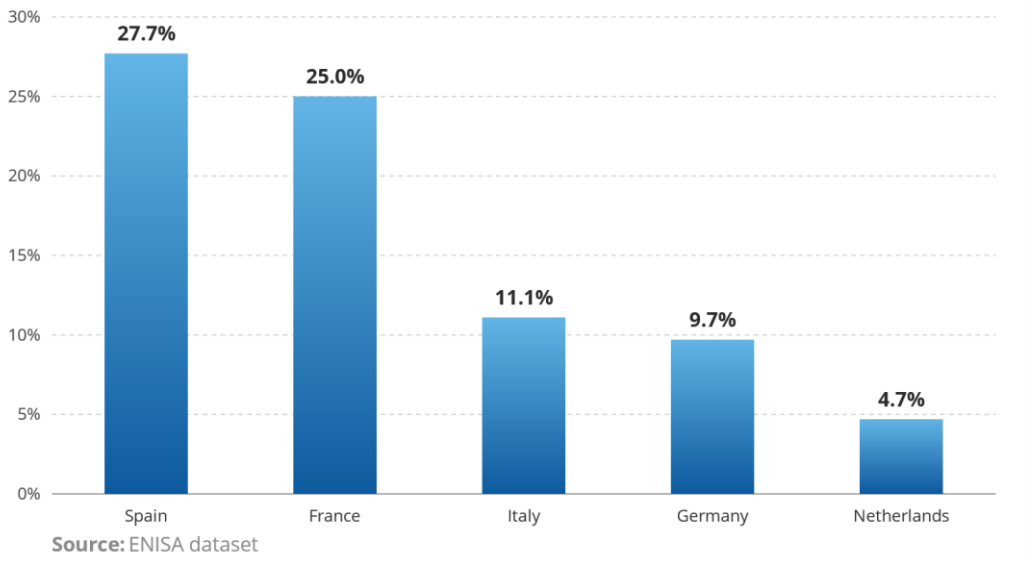


Figure 34 - Top 5 EU MS impacted by data breaches

In May 2025, R0m4nce, reportedly linked to the Hexorcist group, advertised the bulk sale of the source code for more than 1 100 gambling websites on the underground forum DarkForums[189]. The group claimed the package consisted of 4.1 GB of uncompressed PHP code compiled from data dumps dated 15 August 2024 and 30 November 2024. Based on the domains identified, at least 12 EU MSs were allegedly impacted.

[172] https://www.bleepingcomputer.com/news/security/europcar-gitlab-breach-exposes-data-of-up-to-200-000-customers/
[173] hxxps://darkforums.st /
[174] https://www.bleepingcomputer.com/news/security/europcar-gitlab-breach-exposes-data-of-up-to-200-000-customers/
[175] hxxps://darkforums.st/Thread-Source-Code-NVIDIA-Data-Breach-Leaked-
[176] hxxps://darkforums.st/Thread-Source-Code-ENEA-Data-Breach-Leaked-Download
[177] hxxps://t.me/thecrimsoncollective
[178] https://www.bleepingcomputer.com/news/security/europcar-gitlab-breach-exposes-data-of-up-to-200-000-customers/
[179] https://www.redhat.com/en/blog/security-update-incident-related-red-hat-consulting-gitlab-instance
[180] https://www.enea.com/news/press-releases/limited-data-leakage-contained-of-non-production-data/
[181] hxxps://darkforums.st/Thread-Selling-IBAN-LEADS-Germany-France-Spain-Italy--19622
[182] hxxps://darkforums.st/Thread-ABANCA-BANK-20-000-IBAN-LEAD-%F0%9F%87%AA%F0%9F%87%B8
[183] hxxps://darkforums.st/Thread-CAIXA-BANK-151-330K-IBAN-LEAD-%F0%9F%87%AA%F0%9F%87%B8
[184] hxxps://darkforums.st/Thread-Selling-Cabify-Drivers-Database-430K
[185] hxxps://darkforums.st/Thread-Selling-Spanish-Claims-Database-1-5M-Caser-Generali-Mutua-Mapfre-Customers
[186] https://www.brinztech.com/breach-alerts/brinztech-alert-catastrophic-live-admin-access-to-bbva-bank-for-sale-imminent-ransomware-attack-mass-fraud-event/
[187] hxxps://darkforums.st/Thread-SANTANDER-BANK-10-000-IBAN-LEAD-ES?highlight=Banco+Santander
[188] hxxps://darkforums.st/Thread-ING-BANK-2025-21-090-IBAN-LEAD-%F0%9F%87%AA%F0%9F%87%B8
[189] hxxps://darkforums.st/Thread-Source-Code-1158-Gamble-Sites-Source-Code-Packed-Selling - Post was removed

During the reporting period **finance/banking accounted for the largest share of observed data breach activity (15.4%)**, followed by other sectors (14.6%), business services (10.7%), public administration (9.3%) and digital providers (8.3%). Overall, data breach activity mainly affected sectors handling sensitive financial operations and personal data, as well as organisations providing digital and public-facing services.

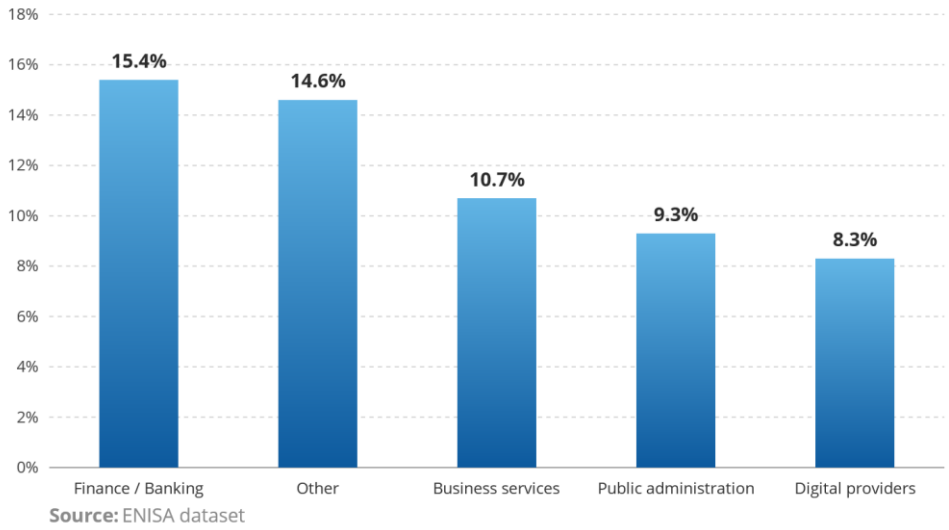


Figure 35 - Top Sectors affected by data breaches

Particularly observed on underground forums and cybercriminal marketplaces used to advertise, leak, or trade compromised data, **data breach claims identified by ENISA primarily originated from the Breached Forums ecosystem** with *darkforums.st* accounting for 58% and *breachforums.st* for 11%. The presence of multiple BreachForums domains reflects the resilience of such platforms to law enforcement disruptions, seizures and closures[190]. Additional activity was identified on *leakbase.la* (8.1%), *xss.is* (6.3%), and *breachforums.bf* (4.3%).

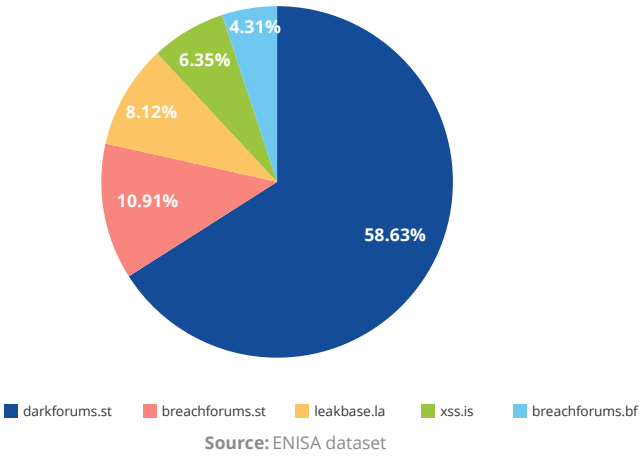


Figure 36 – Breakdown of data breach claims sources

[190] https://www.linkedin.com/pulse/fbi-takes-down-breachforums-notorious-cybercrime-r4g1e/

DATA BREACHES

Data breaches are often claimed as outcomes, providing limited visibility into the Tactics, Techniques and Procedures (TTPs) that led to the compromise. In contrast, ShinyHunters' activities have been documented across the full kill chain, from reconnaissance to the exfiltration, followed by claims, offering a more complete view of this group's tradecraft (see table below)[191]. ShinyHunters (aka ShinyCorp)[192] is a financially motivated group that emerged in 2020, focused on data theft and extortion, targeting cloud and SaaS environments. The group primarily targeted organisations holding sensitive financial, personal and corporate data. Over the reporting period, ShinyHunters used phishing, vishing, credential harvesting, Multi Factor Authentication (MFA) abuse and stolen Open Authentication (OAuth) tokens (T1528 – Steal Application Access Token) to compromise enterprise cloud environments[193]. Observed activity affected platforms including Salesforce, Microsoft 365, SharePoint, Slack, and Google BigQuery[194] (Cloud Infrastructure Discovery (T1580)). They commonly gained access through vishing campaigns impersonating IT personnel to steal Single-Sign-On (SSO) credentials and MFA codes. Following compromise, operators accessed connected SaaS services (Exploitation of Remote Services (T1210) and Software Deployment Tools (T1072)), exfiltrated sensitive data and conducted extortion through their DLS, as well as ransom demands[195] [196] [197] [198].

3.1.3 Ransomware deployments

Ransomware operators continued to disrupt organisations across multiple sectors, through encryption, data theft and extortion-based operations. **The most active ransomware operators in the EU include Qilin, SafePay, Akira, INC Ransom and Hunters International**.

[191] https://socradar.io/blog/dark-web-profile-shinyhunters/
[192] https://www.vectra.ai/modern-attack/threat-actors/shinyhunters
[193] https://cloud.google.com/blog/topics/threat-intelligence/unc6040-proactive-hardening-recommendations
[194] https://reliaquest.com/blog/threat-spotlight-shinyhunters-data-breach-targets-salesforce-amid-scattered-spider-collaboration/
[195] https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion
[196] https://reliaquest.com/blog/threat-spotlight-shinyhunters-data-breach-targets-salesforce-amid-scattered-spider-collaboration/
[197] https://www.mitiga.io/blog/shinyhunters-snowflake-and-rockstar-another-saas-leads-to-compromise
[198] https://www.huntress.com/threat-library/threat-actors/shinyhunters

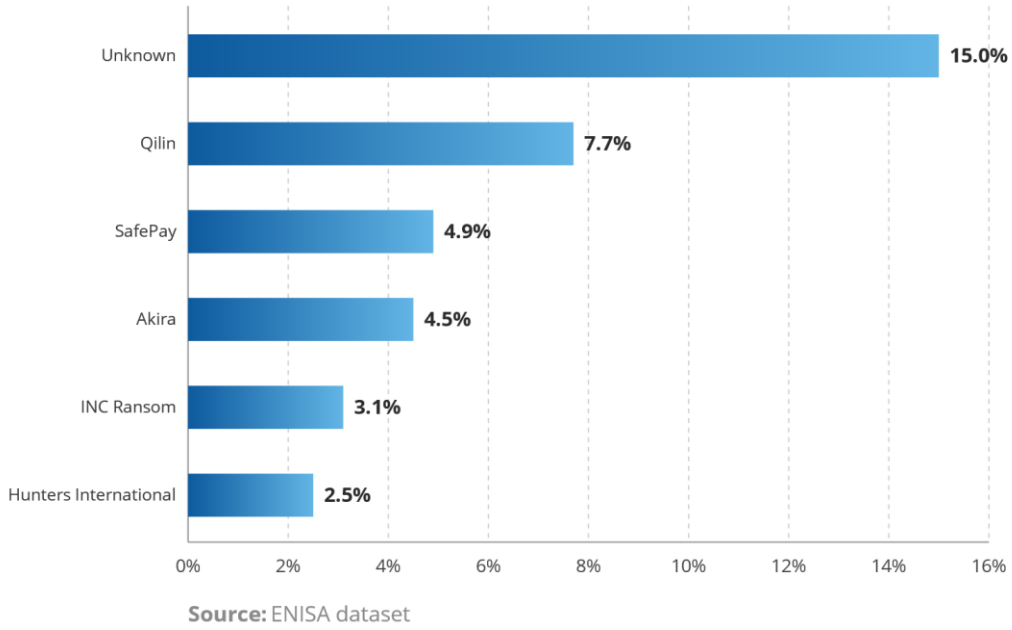


Figure 37 - Top 5 ransomware deployment claims in the EU

Activity during the reporting period showed **fluctuations across the different groups**. Akira entered 2025 with a high tempo of activity, followed by a slight decline in the following months. By contrast Qilin maintained moderate activity levels before recording a significant increase in October 2025. The reason behind this spike could not be identified. Safepay displayed two notable peaks of activity in May 2025 and December 2025, with 22 and 26 claims respectively.

One notable observation concerns Hunters International. One claim was recorded in February 2025, followed by a significant increase to 52 claims in April 2025. While the observed trend towards extortion-only operations may have indicated a transition to Word Leaks ransomware at the time, this hypothesis was not confirmed in the medium-term[199]. Lastly, INC Ransom kept a lower but steady tempo throughout 2025 with monthly claims ranging from 2 to 13.

[199] https://www.group-ib.com/blog/hunters-international-ransomware-group/

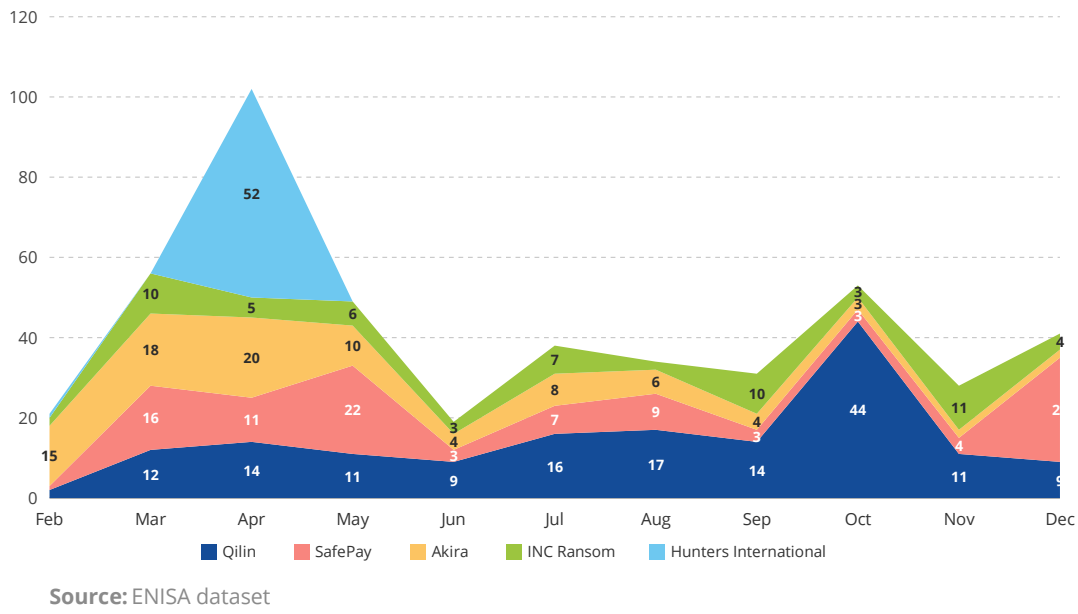


Figure 3830 - Tempo of top ransomware deployments in the EU in 2025

Based on identified **ransomware claims**, **most targeted EU MSs include Germany (26.5%), France (14.7%), Italy (13.6%)**, Spain (12.2%) and the Netherlands (4.7%).While the **least targeted** EU MSs include **Croatia (0,5%), Estonia, Latvia, Bulgaria Slovakia (0,3%) and Lithuania (0,1%)**.

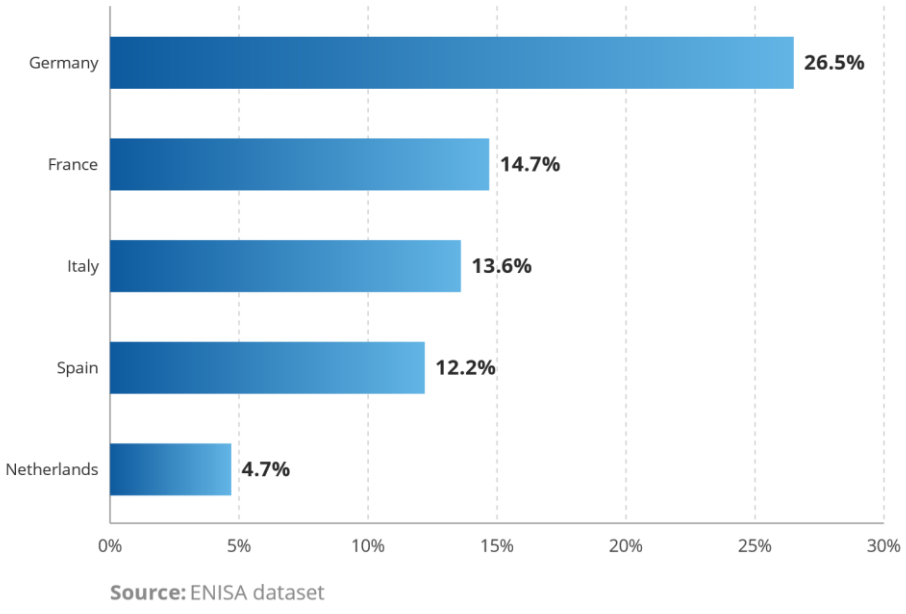


Figure 39 - Top 5 EU MS listed in ransomware claims

While primarily impacting US organisations, SafePay deployments were claimed in the EU, primarily in Germany. Qilin presented more heterogeneous claims against targets located mainly in France, Spain and Italy.

	Qilin	SafePay	Akira	INC Ransom	Hunters International	Total
Germany	4.2%	16.2%	4.8%	5.9%	1.7%	32.8%
France	8.8%	0.2%	0.8%	0.8%	2.1%	12.7%
Spain	6.1%	1.1%	2.9%	0.6%	1.5%	12.2%
Italy	4.0%	0.8%	3.8%	1.3%	1.5%	11.4%
Netherlands	2.1%	0.4%	0.6%	1.1%	0.2%	4.4%
Austria	1.5%	0.4%	0.8%	1.5%	0.2%	4.4%
Belgium	1.1%	0.2%	0.6%	0.4%	1.1%	3.4%
Sweden	1.1%		1.3%	0.6%	0.2%	3.2%
Poland	1.1%	0.2%	0.2%		0.6%	2.1%
Greece	0.2%	0.4%	1.3%	0.2%		2.1%
Ireland	0.6%	0.4%	0.2%	0.2%	0.4%	1.8%
Czechia	0.6%	0.2%		0.4%	0.6%	1.8%
Romania		0.4%	0.2%		0.2%	0.8%
Portugal	0.2%		0.6%			0.8%
Denmark	0.4%		0.4%			0.8%
Cyprus	0.4%			0.2%	0.2%	0.8%
Malta	0.2%		0.4%	0.2%		0.8%
Hungary	0.6%					0.6%
Estonia	0.2%		0.2%			0.4%
Luxembourg	0.2%		0.2%			0.4%
Latvia			0.2%		0.2%	0.4%
Finland		0.4%				0.4%
Croatia	0.2%	0.2%				0.4%
Lithuania					0.2%	0.2%
Bulgaria					0.2%	0.2%

Source: ENISA dataset

Figure 4031 - Top 5 ransomware claims per EU MS

Ransomware deployment for the reporting period covered 47.3% of overall financially motivated activity. The highest share of claimed ransomware deployments was recorded against the **manufacturing sector (25.2%) followed by business services (18.7%), and other (10.7%)**. It is worth noting that within the other sector, most claims were related to the retail/consumer goods subsector. While public administration followed with 6.7%, the heath sector and the production, processing and distribution of food sector ranked next, each accounting for a comparable share of reported claims and completing the list of the most impacted sectors.

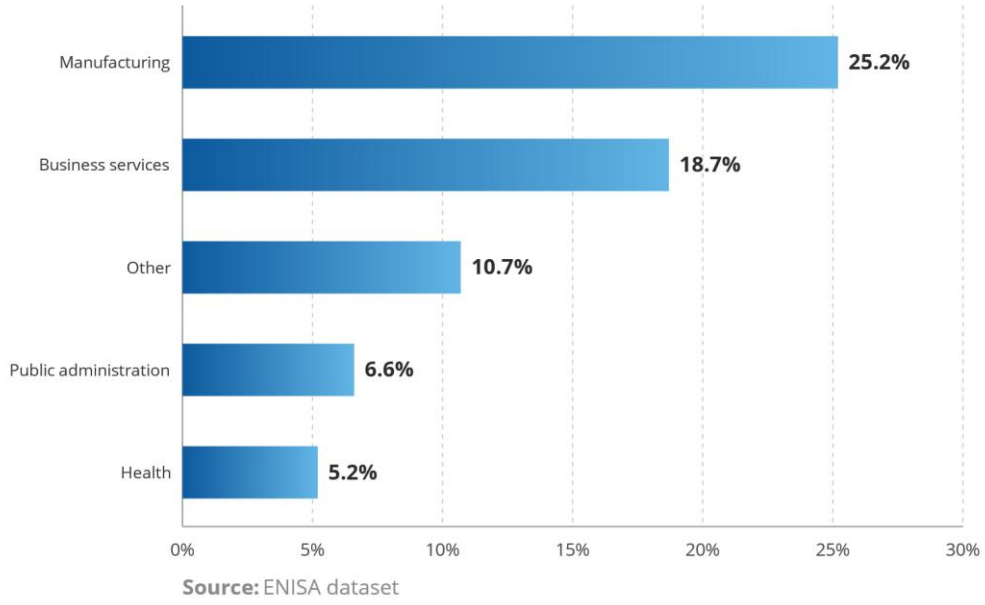


Figure 41 - Top 5 sectors impacted by ransomware claims in the EU

Hereafter is a table showcasing a few ransomware incidents for which an impact was documented to illustrate how ransomware deployments continue to have an impact on operational continuity across sectors and EU MSs over the reporting period.

Date	Title	Brief description	Impact
Mar-25	Qilin ransomware attack on Hospital Los Madroños	Ransomware attack by the Qilin group involving internal network infection, system encryption and data exfiltration[200].	Encryption of files and exfiltration of sensitive personal data (bank accounts, medical histories) of employees, providers and patients; data was published on the group's blog.
May-25	Phantom Mantis (Qilin) Fortinet Campaign	Coordinated intrusion campaign exploiting FortiGate vulnerabilities CVE-2024-21762(EUVD-2025-32142) and CVE-2024-55591(EUVD-2024-52819) for authentication bypass and Remote Code Execution (RCE)[201].	Unauthorised access and ransomware deployment targeting multiple organisations, primarily in Spanish-speaking countries.
May-25	INC ransomware attack targeting Roma Tre University	Roma Tre University's IT infrastructure was targeted by a significant ransomware attack claimed by the INC group, which led to an interruption of the university's digital services[202] [203].	The attack had a widespread impact, rendering websites, student portals and educational platforms (Moodle) inaccessible, while also disrupting essential administrative functions such as accounting, personnel management and internal communication tools.
Jul-25	Ingram Micro Ransomware Incident	Ransomware infection identified on specific internal systems of the global IT distributor[204].	System outage resulting in significant disruptions to order processing and shipping capabilities.
Aug-25	Cl0p Oracle E-Business Suite Exploitation	Exploitation of a zero-day vulnerability CVE-2025-61882(and legacy flaws in Oracle EBS by the Clop ransomware group for pure extortion[205] [206] [207].	Large-scale theft of sensitive data from multiple organisations; followed by extortion demands sent to executives to prevent public data release.
Sept-25	Everest Group Collins Aerospace Hack	Cyberattack by the Everest Group gaining unauthorised FTP access to vMUSE check-in and boarding software infrastructure[208].	Exfiltration of over 1.5 million passenger records and 3 637 airline employee records; caused significant flight disruptions and airport shutdowns across Europe.
Nov-25	Qilin ransomware attack on Francehopital	Cyberattack by the Qilin ransomware group targeting the French healthcare organisation[209].	Potential leak of sensitive healthcare data; threat of data exposure used as leverage to force negotiations.
Dec-25	Slovak Ministry of Economy cyberattack	Ransomware attempt targeting ministry network infrastructure and servers, detected by state cyber units CSIRT and SK-CERT[210].	Potential unauthorised network access; early detection reportedly prevented data encryption or loss.
Dec-25	DroidLock malware campaign	Android ransomware campaign targeting Spanish users via phishing websites, utilising accessibility services to hijack mobile devices[211].	Locking of device screens, credential theft via malicious overlays, and the capability to perform factory resets (total device wipe).

[200] https://hospitallosmadronos.es/aviso-de-ciberseguridad/
[201] https://www.bleepingcomputer.com/news/security/critical-fortinet-flaws-now-exploited-in-qilin-ransomware-attacks/
[202] https://www.uniroma3.it/articoli/attacco-informatico-allinfrastruttura-dellateneo-467162/
[203] https://www.acn.gov.it/portale/documents/20119/923891/operational_summary_may2025_CLEAR_EN.pdf/2062f745-d8d6-e63d-67bf-e5550f70c8bf?t=1770733214823
[204] https://www.businesswire.com/news/home/20250705035732/en/Ingram-Micro-Issues-Statement-Regarding-Cybersecurity-Incident
[205] https://www.theregister.com/2025/10/06/clop_oracle_ebs_zeroday/
[206] https://www.securityweek.com/oracle-e-business-suite-zero-day-exploited-in-cl0p-attacks/
[207] https://cloud.google.com/blog/topics/threat-intelligence/oracle-ebusiness-suite-zero-day-exploitation
[208] https://www.cyberdaily.au/security/12814-exclusive-passenger-and-employee-data-allegedly-compromised-in-collins-aerospace-hack
[209] https://www.dexpose.io/qilin-ransomware-strikes-francehopital/
[210] https://zive.aktuality.sk/clanok/BpJurkm/stat-celi-kyberutoku-je-zavazny-kyberjednotky-zasahuju-na-mieste/
[211] https://zimperium.com/blog/total-takeover-droidlock-hijacks-your-device

To assess the operational behaviour of the most active ransomware operators, ENISA analysed publicly reported TTPs[212] [213] [214] [215] [216]. **The most frequently observed technique was exfiltration over C2 channels (T1041), representing 73.3%.** Techniques related to data encryption for impact, such as T1486, were reported less often (13.7%). This distribution is likely to confirm a **broader operational shift in ransomware activity from encryption-based activity towards data exfiltration** and extortion-focused operations. Ransomware operators were also seen **exploiting vulnerabilities in VPN and firewall appliances**, such as Fortinet (CVE-2024-55591 exploited by Qilin, INC Ransom)[217] [218] and SonicWall or Cisco (CVE-2024-40766 and CVE-2023-20269 exploited by Akira)[219].

While **infostealers** continued to be delivered through cracked software, phishing pages and public code repositories, **new delivery mechanisms to evade detection** were also observed, such as fake CAPTCHA verification pages, cloud-based file hosting services and embedded links in video platforms. A primary initial access vector used by Qilin was the ClickFix tactic, using fake human verification prompts to trick users into installing NetSupport Manager or StealC infostealers, while in some instances they leveraged stolen credentials or conducted brute-force attacks against VPNs (particularly Fortinet devices)[220] [221] [222]. Safepay continued to use a social engineering tactic similar to the one used by Black Basta, during which they impersonate IT staff to load **Remote Management Tools (RMMs)** [223] [224] [225] [226] [227].

Reuse of leaked builders (malware creation tools) continued to be observed, as illustrated by SafePay ransomware, suspected of being derived from a modified LockBit3 builder[228]. It is likely that publication of the VanHelsing RaaS source code in May 2025 will be leveraged by other ransomware operators and contribute to the lowering of barriers of entry to the cybercriminal market for newcomers[229].

Cybercrime groups also continued using tools designed to **disable Endpoint Detection and Response (EDR) solutions**, enabling them to conduct stealthier intrusions focused on rapid data exfiltration. In June 2025, variants of EDRKillShifter started to be incorporated in multiple RaaS toolsets, including Medusa, Qilin, Dragonforce, Lynx, Blacksuit, RansomHub and INC[230] [231] [232] [233]. Another technique illustrating this trend is the exploitation of vulnerable drivers **(Bring Your Own**

[212] https://www.hhs.gov/sites/default/files/qilin-threat-profile-tlpclear.pdf
[213] https://attack.mitre.org/groups/G1032/
[214] info.quorumcyber.com/mr_safepay_ransomware.pdf
[215] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a
[216] https://www.quorumcyber.com/wp-content/uploads/2023/11/QC-Hunters-International-Ransomware-Report-TI.pdf
[217] https://www.sophos.com/en-us/blog/i-am-not-a-robot-clickfix-used-to-deploy-stealc-and-qilin
[218] https://www.hvs-consulting.de/en/blog/inc-ransom-ransomware
[219] https://zensec.co.uk/blog/unmasking-akira-the-ransomware-tactics-you-cant-afford-to-ignore/
[220] https://blog.checkpoint.com/security/lumma-infostealer-down-but-not-out/
[221] https://www.sophos.com/en-us/blog/i-am-not-a-robot-clickfix-used-to-deploy-stealc-and-qilin
[222] https://www.picussecurity.com/resource/blog/qilin-ransomware
[223] https://www.bitdefender.com/en-us/blog/businessinsights/security-advisory-adversaries-abuse-microsoft-teams-and-quick-assist
[224] https://www.bitdefender.com/en-us/blog/businessinsights/safepay-ransomware-attacks-ttps
[225] https://malware.news/t/dark-web-profile-safepay-ransomware/97350
[226] https://www.bitdefender.com/en-us/blog/businessinsights/safepay-ransomware-attacks-ttps
[227] https://malware.news/t/dark-web-profile-safepay-ransomware/97350
[228] https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/safepay-ransomware/
[229] https://x.com/Manu_De_Lucia/status/1924792567461294492
[230] https://news.sophos.com/en-us/2025/08/06/shared-secret-edr-killer-in-the-kill-chain/
[231] https://www.halcyon.ai/blog/edr-killers-increasingly-used-to-bypass-security-in-ransomware-operations
[232] https://www.eset.com/blog/en/business-topics/threat-landscape/stop-edr-killers/
[233] https://www.theregister.com/2025/08/14/edr_killers_ransomware/

Vulnerable Drivers - BYOD) to disable EDR systems[234] [235]. Of particular concern in this regard is the reported abuse of the legitimate tool HRSword[236], used to disable EDR/antivirus agents.

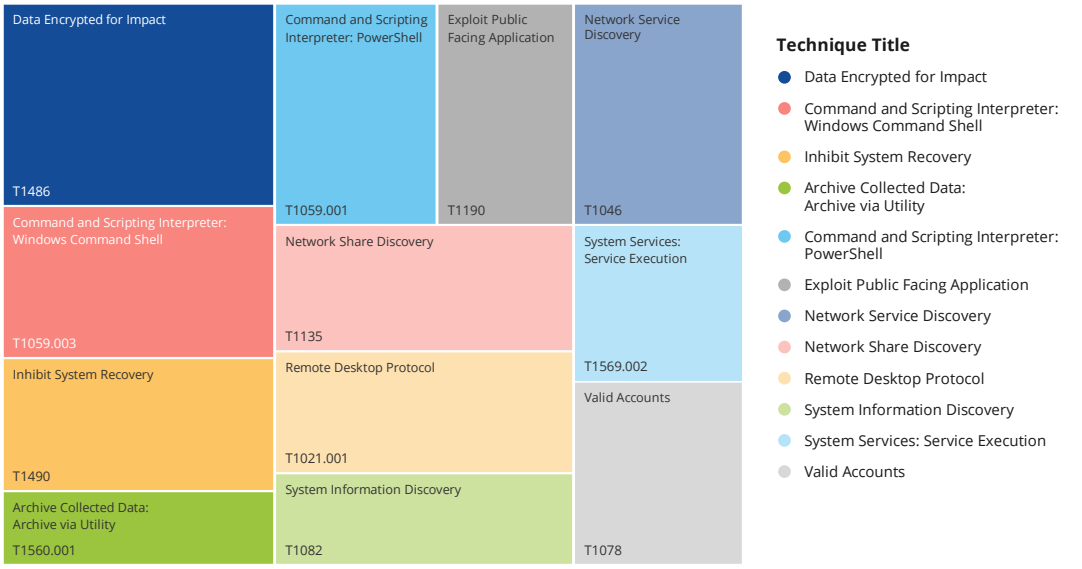
As part of their opsec and stealth efforts, cybercriminals were seen **leveraging legitimate services for C2 purposes, challenging detection and disruption efforts for cyber defenders**[237] [238].

Qilin relied on **aggressive pressure tactics**, including a new 'call lawyer' feature, which mimics legal escalation, pressuring victims to act quickly under the illusion of legal consequences[239] [240]. This technique is particularly relevant in the EU, where cyber incident reporting and GDPR obligations are likely to represent a driver for victims to pay the ransom and avoid reputational damage. In several campaigns, priority was given to complexifying the system recovery process, with the deletion of Volume Shadow Copies[241] [242] or the targeting of Virtual Machine infrastructure[243] [244] [245].

Data exfiltration is typically performed using legitimate file transfer tools such as Rclone[246], FileZilla[247] and Cyberduck to send stolen data to legitimate cloud-storage providers such as Backblaze[248] or MEGA[249]. The table and graphs below present the most commonly seen TTPs mapped with the MITRE ATT&CK framework of most commonly seen ransomware in the EU.

ID	Tactic	Technique Title	Ransomware operators
T1486	**Impact**	**Data Encrypted for Impact**	Akira, Hunters International, INC Ransom, Qilin, Safepay
T1490	**Impact**	**Inhibit System Recovery**	Akira, Hunters International, Qilin, Safepay
T1021.001	**Lateral Movement**	**Remote Desktop Protocol**	Akira, INC Ransom, Qilin
T1190	**Initial Access**	**Exploit Public Facing Application**	Akira, INC Ransom, Qilin
T1046	**Discovery**	**Network Service Discovery**	Akira, INC Ransom, Qilin
T1569.002	**Execution**	**System Services: Service Execution**	Akira, INC Ransom, Qilin
T1082	**Discovery**	**System Information Discovery**	Akira, INC Ransom, Qilin
T1078	**Initial Access**	**Valid Accounts**	Akira, INC Ransom, Qilin
T1059.003	**Execution**	**Command and Scripting Interpreter: Windows Command Shell**	Akira, INC Ransom, Qilin, Safepay
T1560.001	Collection	Archive Collected Data: Archive via Utility	Akira, INC Ransom, Safepay
T1059.001	Execution	Command and Scripting Interpreter: PowerShell	Akira, Qilin, Safepay
T1135	Discovery	Network Share Discovery	Hunters International, INC Ransom, Safepay
T1041	Exfiltration	Exfiltration over C2 channels	Akira, Hunters International, INC Ransom, Qilin, Safepay
T1486	Impact	Data Encrypted for Impact	Akira, Hunters International, INC Ransom, Qilin, Safepay

[234] https://www.elastic.co/security-labs/abyssworker
[235] https://www.ic3.gov/CSA/2025/251113.pdf
[236] https://www.theregister.com/2025/03/31/ransomware_crews_edr_killers/
[237] https://malware.news/t/fake-wordpress-domain-renewal-phishing-email-stealing-credit-card-and-3-d-secure-otp/102920
[238] https://www.resecurity.com/blog/article/chinese-threat-nfc-enabled-fraud-in-the-philippines-financial-sector
[239] https://thehackernews.com/2025/06/qilin-ransomware-adds-call-lawyer.html
[240] https://www.s-rminform.com/latest-thinking/ransomware-in-focus-meet-qilin
[241] https://www.ic3.gov/CSA/2025/251113.pdf
[242] https://www.picussecurity.com/resource/blog/qilin-ransomware
[243] https://www.ic3.gov/CSA/2025/251113.pdf
[244] https://www.picussecurity.com/resource/blog/qilin-ransomware
[245] https://www.ic3.gov/CSA/2025/251113.pdf
[246] https://www.ic3.gov/CSA/2025/251113.pdf
[247] https://malware.news/t/dark-web-profile-safepay-ransomware/97350
[248] https://blog.talosintelligence.com/uncovering-qilin-attack-methods-exposed-through-multiple-cases
[249] https://www.ic3.gov/CSA/2025/251113.pdf



Source: ENISA dataset

Figure 322 - Common TTPs used by the top ransomware operators

The first half of 2025 saw several RaaS shutdowns, including BlackBasta in February[250] and RansomHub in April 2025[251]. In March 2025, DragonForce's announcement that RansomHub was joining its cartel was identified by researchers as a hostile takeover, rejected by RansomHub operators. Of note, DragonForce was operating its own RansomBay white-label service to allow affiliates to rebrand the ransomware under a different name[252]. LockBit operations were impacted by the compromise, defacement and leaking of their affiliate management panel, and since May 2025 the group seems to have ceased its activities[253]. Whether the newly documented LockBit4 operator Syrphid is a former LockBit affiliate is not known at the time of reporting[254].

The Babuk2 (aka Bjorka[255]) ransomware operators claimed attacks against military, law enforcement and defence organisations, including in the EU[256] [257] [258]. Through the claimed attacks, it was observed that since mid-March, Babuk2 has been increasingly targeting the defence sector with victims around the globe[259] [260] [261]. Since resurfacing in January 2025, Babuk2 is assessed to be a copycat of Babuk, notably **fabricating or recycling ransomware claims made by other ransomware operators**[262] [263] [264]. Additionally, Babuk2 shifted towards selling access to compromised enterprise networks on

[250] https://www.threatdown.com/blog/infighting-brings-down-the-black-basta-ransomware-group/
[251] https://www.infosecurity-magazine.com/news/ransomware-fall-april-ransomhub/
[252] https://www.infosecurity-magazine.com/news/dragonforce-turf-war-ransomware/
[253] https://socradar.io/blog/lockbit-hacked-60000-bitcoin-addresses-leaked/
[254] https://www.broadcom.com/support/security-center/protection-bulletin/lockbit-4-0-ransomware
[255] https://www.guidepointsecurity.com/blog/ongoing-report-babuk2-babuk-bjorka/
[256] https://x.com/TMRansomMon/status/1907710849222918232
[257] hxxp://bxwu33iefqfc3rxigynn3ghvq4gdw3gxgxna5m4aa3o4vscdeeqhiqad.onion/blog/f97ccef2d86837e857d474e38711b9a9edf80a009c95b361cc70e175464125cf
[258] https://undercodenews.com/rheinmetall-hit-by-babuk2-ransomware-group-what-we-know-so-far/
[259] https://www.hendryadrian.com/ransom-turkish-defense-military
[260] https://www.redpacketsecurity.com/babuk2-ransomware-victim-baykar-turkish-defense-company-c4i-and-artificial-intelligence/
[261] https://www.hendryadrian.com/ransom-secret-plans-of-indian-army/
[262] https://www.cyjax.com/resources/blog/babuk-ba-back-potential-return-of-the-infamous-raas-group/
[263] https://gbhackers.com/babuk2-ransomware-issues-fake-extortion-demands-using-data/
[264] https://cyberpress.org/babuk-locker-selling-access-to-high-profile-targets/

underground forums, functioning partly as an Initial Access Broker (IAB), sometimes repurposing previously published data, hindering the trustworthiness of this group[265].

3.2 Sectoral impact

Cybercrime activity over the reporting period remained opportunistic and affected a broad range of sectors across the EU. Financially motivated operators primarily targeted sectors handling monetizable data. Across all cybercrime incidents, **manufacturing was the most impacted sector (14.4%), followed by business services (13.5%), and other (11%). Finance/banking represented 9.2%, and public administration 8.7%**. It is likely that this ranking stems from multiple factors, possibly including cybersecurity maturity level, opportunity to collect large amounts of data, notably through downstream targeting (third-party attacks)[266].

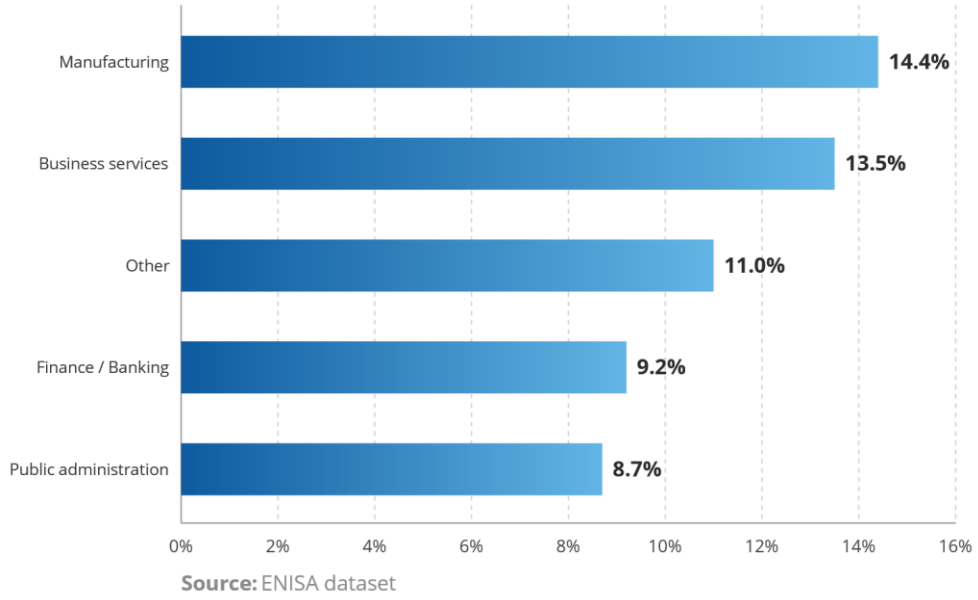


Figure 43 - Top 5 sectors impacted by cybercrime in the EU

3.3 Geographical impact

Throughout 2025, cybercrime impacted organisations across multiple EU MSs, with the highest number of identified financially motivated events observed in **Germany with 18.1%, Spain (17.7%), closely followed by France (17.6%), Italy (12.6%) and the Netherlands (4.6%)**. While this ranking could stem from multiple factors, it is likely these EU MSs would be seen as major economic players within the EU and thus represent high value targets, as analysed by CCB [267].

[265] https://cyberpress.org/babuk-ransomware-group-claims-attack/
[266] https://www.enisa.europa.eu/sites/default/files/2026-05/ENISA%20NIS360%202026.pdf
[267] https://ccb.belgium.be/recent-news-tips-and-warning/richer-country-more-ransomware-victims-it-has?

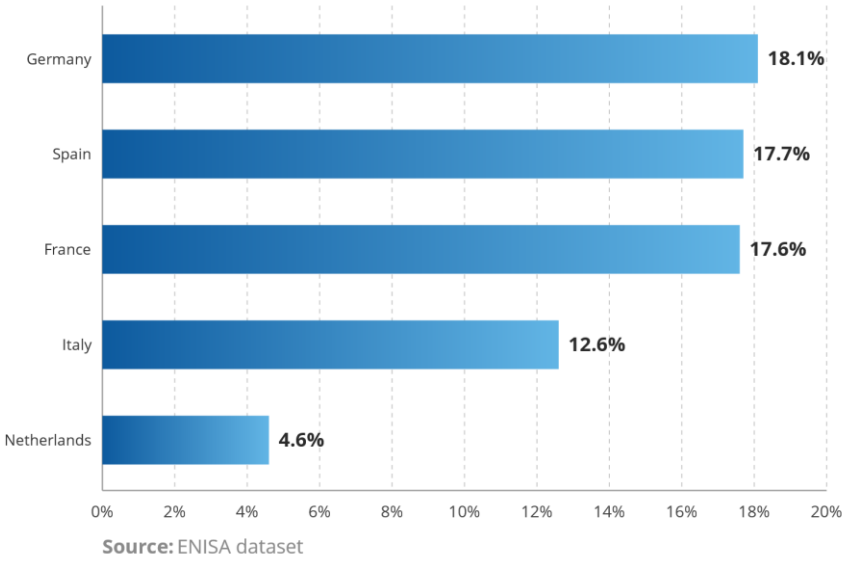


Figure 44 - Top 5 EU MSs impacted by cybercrime incidents

3.4 Key trends

Credential theft activity in 2025 continued to rely on infostealers, which were commonly used to support phishing, fraud, ransomware operations and access brokerage. Public reporting documented continued use of malware families including Lumma, Vidar, Rhadamanthys, Redline, VenomStealer, Stealc and Strela, often delivered through phishing campaigns, ClickFix lures, fake software updates and compromised cloud services [268] [269] [270] [271]. Several campaigns specifically targeted EU users and organisations, including a malspam campaign targeting the Italian pension sector that redirected victims to a fake webmail portal to distribute FormBook, and the ThunderKitty phishing campaign, which used phishing emails as the initial vector to deploy infostealer malware[272] [273]. Reports showed continued use of infostealers to steal credentials, browser data, MFA tokens and session cookies, enabling account takeover and unauthorised access[274] [275].

Leaked Black Basta communications also showed how **credentials obtained through infostealer infections and access brokerage supported ransomware deployment and lateral movement activity**[276] [277]. The reporting period also showed an overlap between phishing, and credential theft operations. Operators combined PhaaS infrastructure, AiTM frameworks and malware payloads to bypass MFA and distribute infostealers through AI-themed lures, fake support interactions and

[268] https://www.proofpoint.com/us/blog/threat-insight/update-fake-updates-two-new-actors-and-new-mac-malware
[269] https://unit42.paloaltonetworks.com/phantomvai-loader-delivers-infostealers/
[270] https://ccb.belgium.be/sites/default/files/2025-11/Xander_%20Fransen_QCTR_Q32025_Belgian_Cyber_Threat_Landscape.pdf
[271] https://www.acn.gov.it/portale/en/w/venomstealer-analisi-tecnica
[272] https://www.acn.gov.it/portale/en/w/campagna-malspam-distribuisce-infostealer
[273] https://www.acn.gov.it/portale/en/w/thunderkitty-campagna-di-phishing-volta-alla-diffusione-di-infostealer
[274] https://www.levelblue.com/blogs/spiderlabs-blog/a-deep-dive-into-strela-stealer-and-how-it-targets-european-countries
[275] https://www.eset.com/blog/en/business-topics/threat-landscape/lumma-stealer-threat/
[276] https://www.theregister.com/special-features/2025/02/21/black-bastas-fighty-internal-chats-leak-online/725906
[277] https://info.ke-la.com/hubfs/Reports/KELA%20Report%20-%20Black%20Basta%20Leak_%20How%20Ransomware%20Operators%20Gain%20Access.pdf

smishing campaigns[278] [279]. The main outcome of these operations remained financial gain through fraud, scams, credential resale and the sale of unauthorised access.

Phishing campaigns continued being seasonal. The impersonation of tax authorities and government digital services were observed in at least nine EU MSs during the reporting period. Operators impersonated national tax agencies and e-government platforms to distribute phishing emails, SMS messages and fraudulent tax refund notifications. Common lures included tax reimbursement claims, overdue payment notices and requests to update identity or banking information. Multiple national authorities issued public warnings regarding ongoing phishing and smishing activities targeting citizens[280] [281] [282] [283] [284] [285] [286] [287] [288] [289]. Italy notably saw several phishing campaigns impersonating government institutions, including the Ministry of Defence, to collect user credentials[290], phishing campaigns abusing trusted financial brands such as PayPal as well as administrative issues such as alleged traffic code violations[291] [292]. Public reporting further highlighted **adaptive phishing campaigns employing encrypted payloads and victim profiling mechanisms** to selectively identify targets, while other campaigns used fake Zoom invitations to deliver ScreenConnect-based RATs[293] [294].

Tycoon 2FA was reportedly the most widely observed phishing kit globally in 2025[295]. The framework operated as an Adversary-in-the-Middle (AiTM) phishing kit designed to bypass multi-factor authentication. Activity linked to Salty 2FA declined from October 2025, while newer samples showed overlapping indicators associated with both Salty 2FA and Tycoon 2FA, potentially indicating operational overlap or shared use linked to the Storm-1747 cluster[296]. Xworm was also deployed as a phishing payload through emails using AI-themed lures, including fake video conferencing invitations and links to compromised cloud storage services targeting corporate environments[297] [298]. In parallel, the Lighthouse phishing framework, linked to the Smishing Triad, enabled large-scale credential harvesting operations. A significant surge in Halloween-themed scams was also reportedly observed during the period between 15 September and 15 October[299].

Domain name registration serves as the primary infrastructure for modern cybercrime, with **77% of phishing domains reportedly being registered specifically to facilitate attacks**. It enables high-volume threats such as phishing kits and ClickFix campaigns, large-scale smishing operations among

[278] https://unit42.paloaltonetworks.com/clickfix-generator-first-of-its-kind/
[279] https://www.huntress.com/blog/fake-anydesk-clickfix-metastealer-malware/
[280] https://sede.agenciatributaria.gob.es/Sede/ayuda/consultas-informaticas/informacion-casos-phishing/2025.html
[281] https://www.incibe.es/ciudadania/avisos
[282] https://www.ertnews.gr/eidiseis/proeidopoiisi-tis-aade-gia-ilektroniki-apati-me-paraplanitika-sms-dithen-apo-myaade-i-gov-gia-foro-kykloforias-ti-einai-to-smishing/
[283] https://info.portaldasfinancas.gov.pt/pt/destaques/Paginas/Alerta_seguranca_20251128.aspx
[284] https://safeonweb.be/fr/actualite/attention-de-faux-messages-concernant-la-declaration-dimpots-circulent
[285] https://safeonweb.be/fr/actualite/avertissement-des-mails-de-phishing-envoyes-au-nom-du-spf-finances
[286] https://www.bmf.gv.at/presse/pressemeldungen/2025/august/phishing-warnung.html
[287] https://www.mein-klagenfurt.at/aktuelle-pressemeldungen/pressemeldungen-september-2025/achtung-phishing-gefaelschte-mails-und-sms-von-id-austria-finanzamt-und-oegk-im-umlauf
[288] https://www.bundesnetzagentur.de/DE/Vportal/Meldungen/Phishing_BZSt_BNetzA.html
[289] https://nki.gov.hu/figyelmeztetesek/tajekoztatas/ado-visszateritesre-hivatkozik-a-nav-nevevel-visszaelo-uj-adathalasz-kampany/
[290] https://www.acn.gov.it/portale/en/w/phishing-mirato-a-enti-governativi
[291] https://www.acn.gov.it/portale/w/phishing-campagna-a-tema-paypal-
[292] https://www.acn.gov.it/portale/en/w/phishing-campagna-a-tema-violazione-codice-della-strada-
[293] https://www.acn.gov.it/portale/w/under-the-hood-analisi-tecnica-di-un-payload-di-phishing-adattivo
[294] https://www.acn.gov.it/portale/w/rat-basato-su-screenconnect-veicolato-da-falsi-inviti-zoom
[295] https://medium.com/@anyrun/malware-trends-overview-report-2025-8aba11baacd3
[296] https://any.run/cybersecurity-blog/salty2fa-tycoon2fa-hybrid-phishing-2025
[297] https://www.microsoft.com/en-us/security/blog/2025/03/13/phishing-campaign-impersonates-booking-com-delivers-a-suite-of-credential-stealing-malware/
[298] https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/malicious-screen-connect-campaign-abuses-ai-themed-lures-for-xworm-delivery/
[299] https://www.bitdefender.com/en-us/blog/hotforsecurity/bitdefender-labs-uncovers-halloween-scams-flooding-inboxes-and-feeds

which Smishing Triad reportedly manages approximately 25 000 active phishing domains in any given eight-day period. Moreover, Hazy Hawk weaponizes misconfigured 'dangling' CNAME records to hijack the reputable subdomains of organisations such as the CDC and various state governments. The frequency of bulk registration services and free dynamic DNS subdomains—which require minimal identity verification—allows criminals to generate disposable, untraceable infrastructure that contributed to a 38% increase in phishing domains over the past year. Consequently, registries and registrars bear a significant responsibility in detecting and mitigating this abuse[300] [301] [302] [303]. Additional TTPs of interest over the reporting period include **the increase of generative AI and deepfake videos**, to impersonate trusted contacts as part of social-engineering efforts. In late 2024, over two million accounts linked to pig-butchering activity were taken down, much of it originating from criminal centres in Southeast Asia and, increasingly, in Eastern Europe and Africa[304] [305] [306].

The theft of cryptocurrencies also keeps on maturing into a highly professionalised system, with cryptocurrency drainers delivered through phishing campaigns, seen increasingly offered as a service (**Drainer-as-a-Service**)[307], allowing cybercriminals to gain control of victims' digital wallets and steal funds. The theft of digital assets via cryptocurrency drainers fluctuated in line with market volatility but remained a persistent and scalable threat, maturing into a CaaS system, particularly as decentralised finance (DeFi) adoption continue growing across the EU. 2025 saw the emergence of Albiriox, an Android trojan seen targeting over 400 global financial and cryptocurrency applications to facilitate **on-device fraud**, primarily focusing on users in Austria[308]. The Jingle Thief campaign uses phishing and smishing to steal credentials after conducting extensive reconnaissance operations allowing them to create highly convincing phishing content[309]. A novel Android malware named SuperCard X enabling **NFC relay attacks** for fraudulent cash-outs was also observed. The malware intercepts and relays NFC communication from compromised devices[310]. Fraudsters on several occasions **contacted** victims **via Messenger or WhatsApp** sharing links to download an application or request payment for a sign-up fee on the same website, leading to phishing and card detail theft[311]. The use of **SIM boxes** to enable fraud further increased. The abuse of SIM boxes provided the hardware for large-scale attacks, enabling online fraud-related crimes such as phishing smishing, and fraudulent account creation[312].

[300] https://alluresecurity.com/blog/dynamic-dns-abuse/
[301] https://www.darkreading.com/endpoint-security/clickfix-attacks-dns-lookup-command-modelorat
[302] https://thehackernews.com/2026/02/microsoft-discloses-dns-based-clickfix.html
[303] https://www.infoblox.com/blog/threat-intelligence/cloudy-with-a-chance-of-hijacking-forgotten-dns-records-enable-scam-actor/
[304] https://about.fb.com/news/2024/11/cracking-down-organized-crime-scam-centers/
[305] https://www.wired.com/story/pig-butchering-scam-invasion/
[306] https://www.europol.europa.eu/media-press/newsroom/news/criminal-phishing-network-resulting-in-over-480-000-victims-worldwide-busted-in-spain-and-latin-america
[307] https://dl.acm.org/doi/10.1145/3730567.3764476
[308] https://www.cleafy.com/cleafy-labs/albiriox-rat-mobile-malware-targeting-global-finance-and-crypto-wallets
[309] https://unit42.paloaltonetworks.com/cloud-based-gift-card-fraud-campaign/
[310] https://www.cleafy.com/cleafy-labs/supercardx-exposing-chinese-speaker-maas-for-nfc-relay-fraud-operation
[311] https://www.threatfabric.com/blogs/datzbro-rat-hiding-behind-senior-travel-scams
[312] https://www.europol.europa.eu/media-press/newsroom/news/cybercrime-service-takedown-7-arrested

Thirty-three EU organisations were identified as targets of repeat victimisation, with activities involving ransomware (44%) and data breaches (40%). It is likely that part of these activities is operationally linked, and that the repeated targeting was enabled by a lack of restoration practices following incident response.

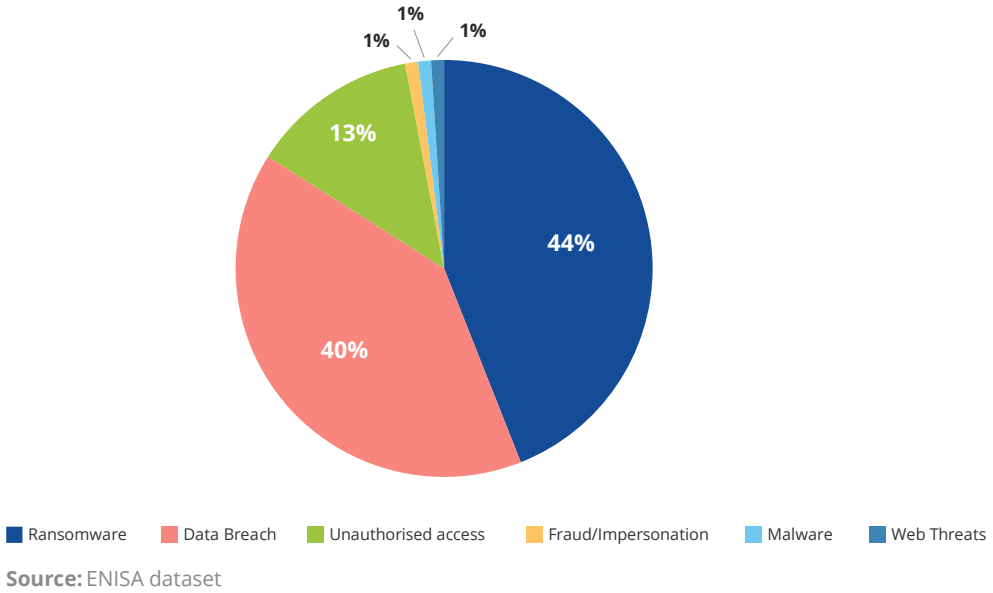


Figure 45 - Type of incidents observed in repeat victimisation cases in the EU

Of rising and significant concern is **the physical targeting, including kidnapping, of individuals involved in the crypto industry, as well as their families**[313] [314]. These events have been linked to data leaks from centralised crypto exchanges, which often contain PII, including, in some cases, home addresses[315]. Such physical attacks were publicly reported in multiple EU MSs, with several high-profile cases in Belgium[316], France[317] and Spain[318].

[313] https://web.archive.org/web/20251208145413/https://cointelegraph.com/news/violent-crypto-robberies-rise-six-attacks-investors
[314] https://web.archive.org/web/20251208132450/https://cointelegraph.com/news/bitcoin-wrench-attacks-to-double-2021-peak
[315] https://web.archive.org/web/20251130085416/https://cointelegraph.com/news/1-bitcoiner-kidnapped-every-week-cyrpto-exec
[316] https://www.bruxellestoday.be/faits-divers/course-poursuite-enlevement-epouse-cryptomonnaies.html
[317] https://www.theguardian.com/world/2025/may/04/french-police-investigate-spate-of-cryptocurrency-millionaire-kidnappings
[318] https://metro.co.uk/2025/02/09/three-british-men-spain-arrested-kidnap-cryptocurrency-broker-22523644/

3.5 Tackling cybercrime in the EU

Activities carried out by law enforcement authorities continued to play a role in the dynamics of the cybercrime environment throughout the reporting period. Joint law enforcement efforts aimed at takedowns of ransomware groups, criminal infrastructure, online marketplaces and services used for assisting malicious activities have been taken as measures for disrupting cybercriminal operations and hindering their capabilities. While the **direct impact of such law enforcement activities can vary greatly and is rarely quantified, they often affect the operating environment** by forcing cybercriminals to adjust their business models **in the short term**. Below is a table of a few law enforcement operations notably led by EU MSs authorities in 2025, expanded in the Appendix.

Date	LEA Action taken	Results / Impact of Operation	Involved countries/entities
28/01/25	OP Talent - Takedown of Cracked and Nulled platforms users in total[319]	2 suspects arrested 17 servers, 12 domains and 50 devices seized Take down of a financial processor	France, Germany, Greece Italy, Romania and Spain, along with Australian Federal Police and US Department of Justice (DoJ) and Federal Bureau of Investigation (FBI)
05/02/25	Arrest of suspect who allegedly participated in over 40 attacks against Spanish Defence Ministry, NATO systems and US Army to access sensitive data[320]	Arrest of the main suspect	Spain, US FBI
10/02/25	Arrest of key figures behind Phobos and 8Base ransomware[321]	27 servers taken down 400+ companies worldwide warned of ongoing attacks No further 8Base claims observed after the operation	Belgium, Czechia, France, Germany, Poland, Romania, Spain, Sweden, Japan, Singapore, Switzerland, Thailand, United Kingdom, US
07/05/25	Operation PowerOFF - Takedown of 6 stresser/booter services[322]	Takedown of 6 major DDoS-for-hire platforms[323] Arrest of 4 individuals Seizure of 9 domains	Poland, Germany, the Netherlands, US
19/05/25	Operation Endgame - Dismantling of key infrastructure behind malware to launch ransomware attacks[324]	300 servers taken down globally neutralizing 650 domains Seizure of EUR 3.5 million in cryptocurrency Neutralisation of seven malware strains	Denmark, France, Germany, Netherlands, UK, Canada, US
27/05/25	Operation Endgame[325]	Dismantling of crypting and Counter Anti-Virus (CAV) services	Finland, the Netherlands, US
23/06/25	Arrest of hacking forum (BreachForums) operators[326]	4 individuals using the online aliases 'ShinyHunters', 'Hollow', 'Noct' and 'Depressed' for their involvement in operating BreachForums	France
07/08/25	Operation Checkmate[327]	Dismantling of BlackSuit ransomware infrastructure	Germany, Lithuania, the Netherlands, US
24/11/25	Shut down of Cryptomixer[328]	Seizure of over 12 TB of data and more than EUR 25 million in Bitcoin	Germany, Switzerland, Europol

[319] https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-takes-down-two-largest-cybercrime-forums-in-world
[320] https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=16448#
[321] https://www.europol.europa.eu/media-press/newsroom/news/key-figures-behind-phobos-and-8base-ransomware-arrested-in-international-cybercrime-crackdown
[322] https://www.europol.europa.eu/media-press/newsroom/news/ddos-for-hire-empire-brought-down-poland-arrests-4-administrators-us-seizes-9-domains
[323] cfxapi, cfxsecurity, neostress, jetstress, quickdown, and zapcut
[324] https://www.europol.europa.eu/media-press/newsroom/news/operation-endgame-strikes-again-ransomware-kill-chain-broken-its-source
[325] https://www.justice.gov/usao-sdtx/pr/websites-selling-hacking-tools-cybercriminals-seized
[326] https://www.bleepingcomputer.com/news/security/breachforums-hacking-forum-operators-reportedly-arrested-in-france/
[327] https://www.ice.gov/news/releases/ice-washington-dc-leads-international-takedown-blacksuit-ransomware-infrastructure
[328] https://www.europol.europa.eu/media-press/newsroom/news/europol-and-partners-shut-down-cryptomixer

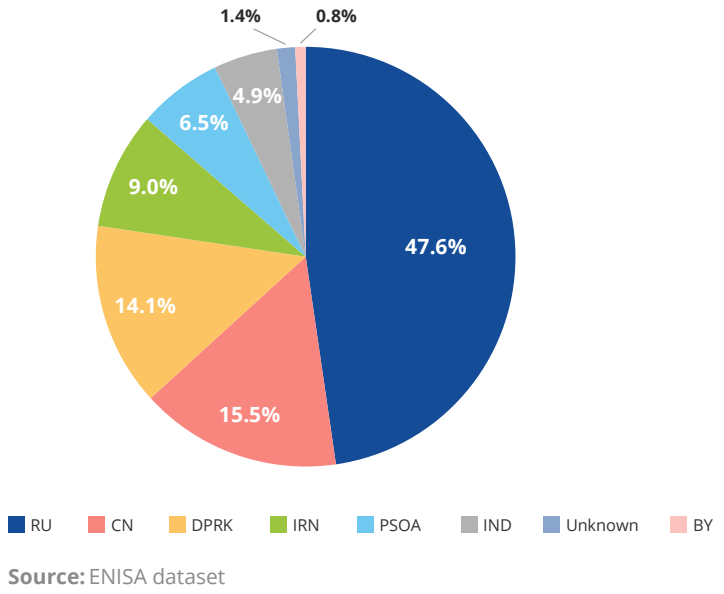
4. State-Nexus Threats

Over the reporting period, the **activities of State-nexus intrusion sets targeting EU MSs remained primarily focused on cyberespionage, strategic intelligence collection and, possibly, intellectual property theft**, notably through the compromise of digital infrastructure and the targeting of public administrations. State-nexus operational activity throughout 2025 was characterised by sustained exploitation of edge infrastructure, the rapid weaponisation of newly disclosed vulnerabilities, the abuse of cloud and identity systems, and the leveraging of social engineering techniques. Civil society within the EU continued being impacted by spyware-enabled targeted surveillance and information operations.

4.1 Key threats

State-nexus intrusion sets were mostly reported to be relying on unauthorised access (81.7%) as well as phishing campaigns (12%). ENISA was able to identify an initial intrusion vector in only 20% of the recorded incidents. Within this subset, vulnerability exploitation was the most frequently observed intrusion vector, accounting for 70% of identified cases. The increase in insider threats (5%) represents a particular concern.

Approximately 1.5% of State-nexus intrusion sets assessed to be carrying out cyberespionage activities against the EU were not imputed to a known nexus. Intrusion sets reportedly associated to Russia accounted for 47.6%, followed by China (15.5%), DPRK (14.1%) and Iran (9%).



Source: ENISA dataset

Figure 336–State-nexus intrusion sets active in the EU by nexus

Russia-nexus intrusion sets continued carrying out cyberespionage campaigns against the public administration, defence and energy sectors in EU MSs, notably through the exploitation of known vulnerabilities and the deployment of bespoke malware. Public administration organisations in multiple EU MSs were targeted, with a specific focus on Ministries of Foreign Affairs and diplomatic entities, as illustrated by campaigns associated to **APT29** or UAC-0063[329]. **APT28** was seen focusing on the EU public administration sector, particularly central governments (please see the top five intrusion sets section). The targeting of defence-related and defence-adjacent organisations was also prevalent throughout the reporting period, with phishing campaigns impersonating defence organisations[330] [331] [332]. A particularly concerning development in Russia-nexus targeting of the EU occurred in December 2025 with a coordinated attack against the energy sector associated to DragonFly, notably involving the use of a wiper[333].

China-nexus intrusion sets continued targeting the EU in 2025, with a consistent focus on telecommunications, maritime, semiconductors, manufacturing and public administration organisations. They also continued their leveraging of vulnerabilities to constitute Operational Relay Boxes (ORBs), including in the EU[334]. Of particular interest is the leveraging of European victims to launch follow-up activities against additional European organisations, as well as against targets in Africa and Southeast Asia[335].

In terms of targeting, open-source reports confirmed that **Salt Typhoon's** targeting of EU organisations started appearing in early 2025[336]. In June, a compromise by the intrusion set was confirmed by Viasat, a global satellite communication company operating across the EU[337]. In August, a joint advisory by multiple EU, US and UK national authorities described operations overlapping with Salt Typhoon against telecommunications, government, transportation and military systems in over 80 countries, including EU MSs[338] [339] [340] [341]. In October, a campaign against an unnamed European telecommunications organisation was associated to Salt Typhoon with moderate confidence[342]. Additional intrusion sets active against the EU notably include **Mustang Panda**, **Liminal Panda, APT31, Ke3chang, PurpleHaze and ShadowPad**[343], **RedNovember**[344] **and UNC6384**[345]. EU victimology was also noted in the reporting on a wave of exploitations targeting on-premises Microsoft SharePoint servers zero-days[346], marking it one of the largest zero-day exploitation campaigns in

[329] https://research.checkpoint.com/2025/apt29-phishing-campaign/
[330] https://cert.gov.ua/article/6284730
[331] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/250521_Sicherheitshinweis_GRU-Einheit_26165.html
[332] CSA_RUSSIAN_GRU_TARGET_LOGISTICS.PDF
[333] https://cert.pl/uploads/docs/CERT_Polska_Energy_Sector_Incident_Report_2025.pdf
[334] https://securityscorecard.com/wp-content/uploads/2025/06/LapDogs-STRIKE-Report-June-2025.pdf
[335] https://research.checkpoint.com/2025/ink-dragons-relay-network-and-offensive-operation/
[336] https://go.recordedfuture.com/hubfs/reports/cta-cn-2025-0213.pdf
[337] https://www.bloomberg.com/news/articles/2025-06-17/viasat-identified-as-victim-in-china-linked-salt-typhoon-hack
[338] https://nukib.gov.cz/cs/infoservis/aktuality/2292-nukib-spolu-s-nsa-a-dalsimi-americkymi-urady-upozornuje-na-cinskeho-aktera-salt-typhoon-ktery-kompromituje-site-po-celem-svete/
[339] https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Sicherheitshinweis_SALT-TYPHOON_250527.html
[340] https://media.defense.gov/2025/Aug/22/2003786665/-1/-1/0/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.PDF
[341] https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4287371/nsa-and-others-provide-guidance-to-counter-china-state-sponsored-actors-targeti/
[342] https://www.darktrace.com/blog/salty-much-darktraces-view-on-a-recent-salt-typhoon-intrusion
[343] https://www.sentinelone.com/labs/follow-the-smoke-china-nexus-threat-actors-hammer-at-the-doors-of-top-tier-targets/
[344] https://www.recordedfuture.com/research/rednovember-targets-government-defense-and-technology-organizations
[345] https://arcticwolf.com/resources/blog/unc6384-weaponizes-zdi-can-25373-vulnerability-to-deploy-plugx/
[346] CVE-2025-49706 (EUVD-2025-20552), CVE-2025-49704 (EUVD-2025-20554), CVE-2025-53770 (EUVD-2025-21981), and CVE-2025-53771 (EUVD-2025-22040)

recent years, with up to eighty countries impacted globally including in the EU by multiple intrusion sets, notably **APT31**[347] [348] [349].

In May 2025, Forescout imputed exploitation of a critical SAP NetWeaver vulnerability CVE-2025-31324 (EUVD-2025-11987) in the EU to **Chaya_004**[350]. Interestingly, the SAP NetWeaver vulnerability was also leveraged by **UNC5221** to target critical infrastructure in the UK, US and Saudi Arabia[351]. In the EU, UNC5221 was separately reported leveraging an exploit chaining two critical Ivanti vulnerabilities to extract sensitive information—such as Office 365 tokens, mobile device credentials, and email configuration files[352].

Throughout 2025, **DPRK-nexus intrusion sets remained particularly active across the EU, conducting cyberespionage and financially motivated employment-themed campaigns** to target organisations with a particular focus on digital infrastructure organisations. This is notably illustrated through the DeceptiveDevelopment campaign, which targeted freelance software developers on job-hunting websites globally, including in the EU, as well as the increased number of reported activities associated to Famous Chollima, notably seeking employment within Western companies operating in the technology, services, defence and government sectors in EU MSs. Lazarus was also reported conducting campaigns related to employment notably targeting EU MSs[353] [354]. The same group also showed an interest in targeting aerospace and defence companies in central and south-eastern Europe, likely as a continuation of their long-running DreamJob campaign[355].

Reports on the activities of Iran-nexus intrusion sets against EU MSs steadily increased in the second and third quarters of 2025. While it is not clear whether this is related to an actual increased tempo of activity or increased numbers of publications in open sources, it is likely related to the 12-day war between Israel and Iran, and the subsequent geopolitical instability in the region[356]. **MuddyWater** reportedly conducted a campaign targeting financial executives across multiple sectors globally, including in the EU[357] [358] [359], and was further noted targeting government and non-profit organisations, including by the use of lures impersonating an EU government[360]. **Charming Kitten** reportedly targeted a Member of the European Parliament (MEP), who acts as chair of the EU–Iran delegation[361], and the Senator of Justice to the city of Berlin[362] [363]. **Nimbus Manticore** was noted in multiple instances targeting defence, telecommunications and aviation sectors in the EU[364] [365] [366], with the

[347] https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/
[348] https://research.eye.security/sharepoint-under-siege/
[349] https://blog.checkpoint.com/research/sharepoint-zero-day-cve-2025-53770-actively-exploited-what-security-teams-need-to-know/
[350] https://www.forescout.com/blog/threat-analysis-sap-vulnerability-exploited-in-the-wild-by-chinese-threat-actor/
[351] https://blog.eclecticiq.com/china-nexus-nation-state-actors-exploit-sap-netweaver-cve-2025-31324-to-target-critical-infrastructures
[352] https://blog.eclecticiq.com/china-nexus-threat-actor-actively-exploiting-ivanti-endpoint-manager-mobile-cve-2025-4428-vulnerability
[353] https://blog.sekoia.io/clickfake-interview-campaign-by-lazarus/
[354] https://www.orangecyberdefense.com/global/blog/cert-news/a-pain-in-the-mist-navigating-operation-dreamjobs-arsenal
[355] https://www.welivesecurity.com/en/eset-research/gotta-fly-lazarus-targets-uav-sector/
[356] https://www.france24.com/en/tag/israel-iran-war/
[357] https://hunt.io/blog/apt-muddywater-deploys-multi-stage-phishing-to-target-cfos
[358] https://www.trellix.com/blogs/research/cfo-spear-phishing-netbird-attack/
[359] https://www.amf-france.org/fr/actualites-publications/actualites/lautorite-des-marches-financiers-met-en-garde-les-professionnels-contre-une-vague-dutilisation
[360] https://x.com/ClearskySec/status/1922298090528375118
[361] https://www.politico.eu/article/european-parliament-iran-delegation-chair-victim-tehran-linked-hacking-hannah-neumann/
[362] https://www.spiegel.de/politik/deutschland/cyberattacke-auf-berliner-justizsenatorin-hacker-stehlen-daten-von-cdu-politikerin-felor-badenberg-a-61e4c099-8306-43b6-a618-cb4141d22036
[363] https://www.tagesschau.de/inland/regional/berlin/hacker-erbeuten-persoenliche-daten-von-justizsenatorin-badenberg-100.html
[364] https://research.checkpoint.com/2025/nimbus-manticore-deploys-new-malware-targeting-europe/
[365] https://www.darkreading.com/cybersecurity-operations/iran-nexus-threat-actor-unc1549-takes-aim-aerospace
[366] https://catalyst.prodaft.com/public/report/modus-operandi-of-subtle-snail/

latter also allegedly targeted by **Chafer**[367]. Finally, **Homeland Justice** was documented targeting the diplomatic missions of at least 10 EU MSs in what was assessed as a broader regional cyberespionage effort aimed at diplomatic and governmental entities during a time of heightened geopolitical tensions[368].

2025 continued seeing the targeting of EU citizens and EU-based individuals through the abuse of tools commercialised by Private Sector Offensive Actors (PSOA). This is notably illustrated by the deployment of Paragon Solutions' **Graphite** spyware through the use of zero-day vulnerabilities to target individuals globally, including in the EU[369] [370] [371] [372] [373] [374] [375]. Infections involving the abuse of **Candiru** were also reported[376]. Another prevalent highlight was the continuous involvement of EU based organisations and EU individuals with PSOA, as reflected through the activities of Intellexa and Altamides[377] [378] [379] [380] [381] [382]. Multiple EU MSs continued actively investigating and prosecuting the abuse of commercial government-grade spyware[383] [384] [385] [386] [387].

Among State-nexus adversaries, **52 distinct intrusion sets were observed to be active in the EU over the reporting period**. The top five identifiable intrusion sets throughout the reporting period included Storm-2372, APT28, Famous Chollima, Calisto and Patchwork, based on the number of EU MSs targeted. Of note, this ranking is highly likely inflated by the breakdown of victimology breakdown accessible to ENISA at the time of writing and **mostly speaks to a lack of stealth** from listed intrusion sets rather than the long-term strategic threat they pose to EU MS organisations.

[367] https://blog.narimangharib.com/posts/2025%2F07%2F1752917718209?lang=en
[368] https://dreamgroup.com/blog/turbid-currents-muddywater-attribution
[369] https://www.theguardian.com/technology/2025/jan/31/whatsapp-israel-spyware
[370] https://www.governo.it/it/articolo/nota-di-palazzo-chigi/27601
[371] https://therecord.media/italy-paragon-spyware-targeted-european-victims-whatsapp
[372] https://cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-010/
[373] https://citizenlab.ca/2025/06/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted/
[374] https://documenti.camera.it/_dati/leg19/lavori/documentiparlamentari/IndiceETesti/034/004/INTERO.pdf
[375] https://techcrunch.com/2025/11/06/italian-political-consultant-says-he-was-targeted-with-paragon-spyware/
[376] https://assets.recordedfuture.com/content/dam/insikt-report-pdfs/2025/cta-2025-0805.pdf
[377] https://go.recordedfuture.com/hubfs/reports/cta-2025-0612.pdf
[378] https://www.icij.org/investigations/cyprus-confidential/predator-spyware-firm-intellexa-resurgent-after-u-s-sanctions/
[379] https://securitylab.amnesty.org/latest/2025/12/intellexa-leaks-predator-spyware-operations-exposed/
[380] https://www.lighthousereports.com/investigation/surveillance-secrets/
[381] https://www.lighthousereports.com/methodology/surveillance-secrets-explainer/
[382] https://www.derstandard.at/story/3100000291834/big-brother-aus-oesterreich-die-firma-die-handys-weltweit-ueberwachte
[383] https://www.diplomatie.gouv.fr/en/presse-et-ressources/decouvrir-et-informer/actualites/communique-conjoint-de-la-france-et-du-royaume-uni-sur-la-conference-de-paris-du-processus-de-pall
[384] https://therecord.media/commercial-spyware-meeting-un-security-council-members
[385] https://vsquare.org/how-a-czech-supply-chain-feeds-the-global-spyware-machine/
[386] https://notesfrompoland.com/2025/03/31/court-rejects-request-to-detain-polish-justice-minister-ziobro-as-part-of-pegasus-investigation/
[387] https://iridia.cat/en/three-executives-of-the-nso-group-charged-for-their-responsibility-in-the-pegasus-espionage-case/

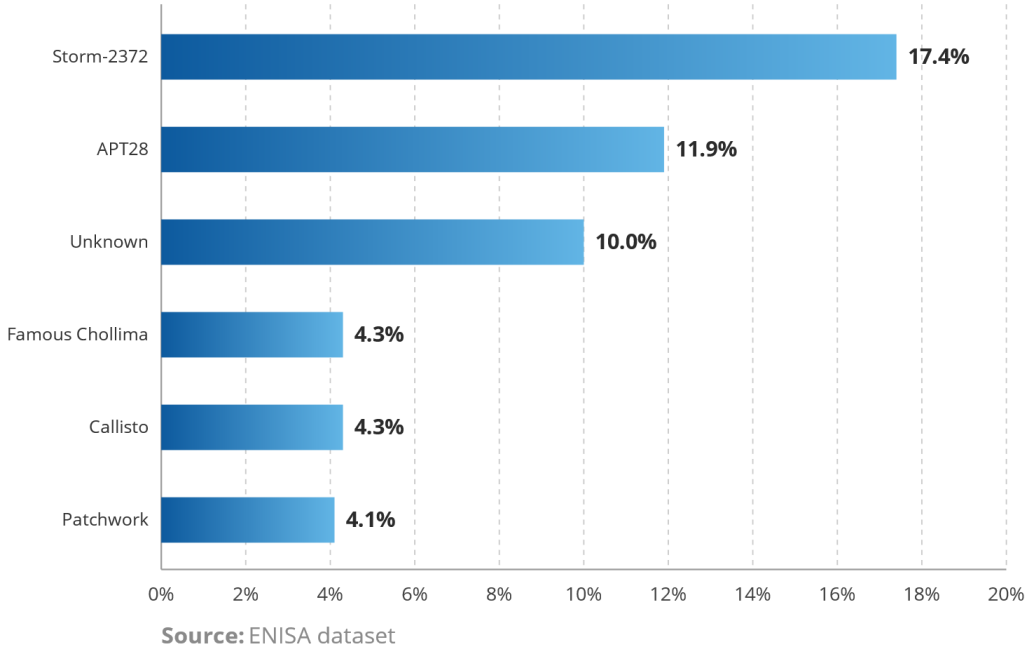


Figure 347 - Top 5 State-nexus intrusion sets active in the EU

In February 2025, Microsoft reported on a large-scale phishing campaign carried out by **Russia-nexus Storm-2372** targeting government, non-governmental organisations (NGOs), information technology (IT) services and technology, defence, telecommunications, health, education, and energy or oil and gas notably in the EU[388]. This campaign was characterised by the use of the device code phishing technique, notably leveraging phishing lures masquerading as WhatsApp, Signal and Microsoft Teams, to entice targeted victims to log into apps, enabling token exfiltration to gain access to compromised accounts. This campaign was aligned with activities carried out by UTA0307 masquerading as a member of the European Parliament on the Committee on Foreign Affairs, reaching out to individuals with personalised emails, requesting a Microsoft Teams meeting to discuss relations between the US and the EU. Whether these two intrusion sets are congruent is not known at the time of writing, as they were handled as two different groups.

Throughout 2025, **Russia-nexus APT28** was seen conducting sustained cyberespionage activities against EU MSs. The intrusion set displayed particular interest in targeting public administration and defence related organisations[389]. Linked to APT28 with moderate confidence, UAC-0063 was seen shifting its initial focus on Central Asian targets[390] to EU-based embassies[391] [392]. In May 2025, a joint advisory from national cybersecurity authorities in Czechia, France, Denmark, Estonia, Germany, and the Netherlands confirmed targeted logistics companies and IT suppliers focused on supply chains, defence contractors and communications infrastructure across the EU since at least 2022, with multiple confirmed targets being involved in providing humanitarian or military assistance to Ukraine[393] [394]. In campaigns targeting EU MSs, APT28 was seen leveraging spear phishing, impersonating or

[388] https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/
[389] https://go.crowdstrike.com/2025-threat-hunting-report.html
[390] https://blog.sekoia.io/double-tap-campaign-russia-nexus-apt-possibly-related-to-apt28-conducts-cyber-espionage-on-central-asia-and-kazakhstan-diplomatic-relations/
[391] https://www.bitdefender.com/en-us/blog/businessinsights/uac-0063-cyber-espionage-operation-expanding-from-central-asia
[392] https://assets.recordedfuture.com/insikt-report-pdfs/2024/CTA-RU-2024-1121.pdf
[393] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/250521_Sicherheitshinweis_GRU-Einheit_26165.html
[394] https://media.defense.gov/2025/May/21/2003719846/-1/-1/0/CSA_RUSSIAN_GRU_TARGET_LOGISTICS.PDF

masquerading as originating from public administration and defence related organisations[395], as well as credential brute-forcing. The intrusion set was also documented leveraging several high-severity vulnerabilities, including CVE-2023-23397 (EUVD-2023-27497) in Outlook, CVE-2020-12641 (EUVD-2020-4942), CVE-2020-35730 (EUVD-2020-23386) and CVE-2021-44026 (EUVD-2021-30885) to gain higher privileges and deploy custom malware HEADLACE and MASEPIE backdoors. Another illustration of APT28 TTPs is the use of NATO-themed spear phishing messages to deliver malware variants BEARDSHELL and SlimAgent[396]. The group was also seen leveraging the Signal messaging application to deploy the recent NotDoor malware[397] [398] [399].

Russia-nexus Callisto targeted at least five EU MSs. The intrusion set was notably seen leveraging a malware named LOSTKEYS[400] [401] designed to extract documents and system data from NGOs, journalists, and Ukraine-aligned individuals and advisors. Additional activities observed in the EU include a phishing and a credential harvesting campaign, targeting government, aerospace and defence, telecom and scientific research industries. In December 2025, Callisto was reported targeting the French NGO Reporters Sans Frontieres through spearphishing in March of that same year[402]. Three GRU officers suspected to have been Calisto operators were included in the European Council list of sanctions announced in December 2025[403].

DPRK-nexus Famous Chollima remained one of the most active intrusion sets in the EU, with activities blending cyber-enabled operations and physical access through employment fraud and was assessed to be pursuing a dual objective of revenue generation and cyberespionage. The intrusion set was seen becoming more active in Europe likely due to increased scrutiny and sanctions by US authorities[404] [405] [406] [407]. The group was active against the digital services provider sector, government and defence-related organisations and the finance vertical. Famous Chollima notably conducted AI-enabled social engineering with fictitious LinkedIn profiles with generative AI-created text and fake profile images[408] [409] [410]. In addition to job applications notably impersonating EU nationals, Famous Chollima was reported leveraging fictitious companies[411] [412]. In terms of TTPs, Famous Chollima reportedly updated their toolset with OtterCookie (v5) implementing JavaScript-based keylogging and screenshotting, reducing the threat actor's reliance on Python distributions[413]. Additionally, they continued the exploitation of the developer ecosystem by using malicious VS Code extensions and trojanized NPM packages, such as Chessfi. The intrusion set was also seen leveraging fictitious companies, as well as C2 infrastructure administered through VPN proxies, and RDP sessions from Russian IP ranges[414] [415] [416].

[395] https://blog.sekoia.io/apt28-operation-phantom-net-voxel/
[396] https://cert.gov.ua/article/6284730
[397] https://blog.sekoia.io/apt28-operation-phantom-net-voxel/
[398] https://lab52.io/blog/analyzing-notdoor-inside-apt28s-expanding-arsenal/
[399] https://www.splunk.com/en_us/blog/security/notdoor-insights-a-closer-look-at-outlook-macros-and-more.html
[400] https://cloud.google.com/blog/topics/threat-intelligence/new-malware-russia-coldriver
[401] https://www.sentinelone.com/labs/phantomcaptcha-multi-stage-websocket-rat-targets-ukraine-in-single-day-spearphishing-operation/
[402] https://blog.sekoia.io/ngo-reporters-without-borders-targeted-by-calisto-in-recent-campaign/
[403] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202502572
[404] https://go.crowdstrike.com/2025-global-threat-report.html
[405] https://assets.recordedfuture.com/insikt-report-pdfs/2025/cta-nk-2025-0213.pdf
[406] https://cloud.google.com/blog/topics/threat-intelligence/dprk-it-workers-expanding-scope-scale/
[407] https://www.justice.gov/opa/pr/two-north-korean-nationals-and-three-facilitators-indicted-multi-year-fraudulent-remote
[408] https://openai.com/global-affairs/disrupting-malicious-uses-of-ai/
[409] https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai
[410] https://reports.dtexsystems.com/DTEX-Exposing+DPRK+Cyber+Syndicate+and+Hidden+IT+Workforce.pdf
[411] https://6068438.fs1.hubspotusercontent-na1.net/hubfs/6068438/saja-dprk-employment-scam-network.pdf
[412] https://news.sophos.com/en-us/2025/05/08/nickel-tapestry-expands-fraudulent-worker-operations/
[413] https://blog.talosintelligence.com/beavertail-and-ottercookie/
[414] https://6068438.fs1.hubspotusercontent-na1.net/hubfs/6068438/saja-dprk-employment-scam-network.pdf
[415] https://news.sophos.com/en-us/2025/05/08/nickel-tapestry-expands-fraudulent-worker-operations/
[416] https://www.trendmicro.com/en_be/research/25/d/russian-infrastructure-north-korean-cybercrime.html

India-nexus Patchwork activity in 2025 focused on large-scale yet temporary spear phishing campaigns targeting diplomatic entities. The intrusion set was notably seen leveraging lures pertaining to China and defence and military topics.

While not included in the top five, China-nexus Mustang Panda still represents a significant threat to EU MS organisations, based on their advanced capabilities and sustained tempo of activity against maritime transportation and public administration. Mustang Panda was notably seen targeting maritime entities in at least four EU MSs and was reported targeting EU MS governmental organisations[417] [418]. In terms of TTPs, the intrusion set was seen leveraging spear phishing as well as compromised USB devices[419] [420] as initial intrusion vectors, as well as DLL sideloading[421] [422]. The intrusion set's malware toolset seen in the EU includes DOPLUGS, Korplug loader, and customized PlugX variants[423], as well as advanced defence evasion and persistence mechanisms[424]. Of note, Mustang Panda was reportedly seen leveraging RA ransomware in Asia, as well as the NailaoLocker in Europe[425] [426] [427].

Of note also is DPRK-nexus intrusion set Kimsuky, active since at least 2012, and seen conducting spear phishing attempts targeting EU MS embassies, particularly in Q2 and Q3, likely in the context of the expansion of the intrusion set's targeting documented in early 2025[428]. Masquerading as diplomatic entities, the intrusion set demonstrated a particular focus on targeting EU MS diplomatic missions, by notably impersonating a secretary of an EU delegation, as well as leveraging documents mimicking correspondence from the embassy of an EU MS. The intrusion set leveraged GitHub as a C2 channel and distributed a variant of XenoRAT relying on cloud storage solutions such as Dropbox and Daum[429].

[417] https://cert.ssi.gouv.fr/uploads/CERTFR-2026-CTI-003.pdf
[418] https://ccb.belgium.be/open-media/1218/download?inline.
[419] https://www.trendmicro.com/en_us/research/24/b/earth-preta-campaign-targets-asia-doplugs.html
[420] https://www.trendmicro.com/en_no/research/25/b/earth-preta-mixes-legitimate-and-malicious-components-to-sidestep-detection.html
[421] https://arcticwolf.com/resources/blog/unc6384-weaponizes-zdi-can-25373-vulnerability-to-deploy-plugx/
[422] https://cloud.google.com/blog/topics/threat-intelligence/prc-nexus-espionage-targets-diplomats
[423] https://www.trendmicro.com/en_us/research/24/b/earth-preta-campaign-targets-asia-doplugs.html
[424] https://www.trendmicro.com/en_no/research/25/b/earth-preta-mixes-legitimate-and-malicious-components-to-sidestep-detection.html
[425] https://unit42.paloaltonetworks.com/ra-world-ransomware-group-updates-tool-set/
[426] https://www.trendmicro.com/en_us/research/25/b/updated-shadowpad-malware-leads-to-ransomware-deployment.html
[427] https://www.orangecyberdefense.com/global/blog/cert-news/meet-nailaolocker-a-ransomware-distributed-in-europe-by-shadowpad-and-plugx-backdoors
[428] https://www.proofpoint.com/us/blog/threat-insight/ta406-pivots-front
[429] https://www.trellix.com/blogs/research/dprk-linked-github-c2-espionage-campaign/

4.2 Sectoral impact

As mentioned in the previous section, State-nexus activities in the EU continued being **prevalent against public administration (29.4%)**, followed by the targeting of manufacturing (9.8%), digital infrastructure (8.2%) civil society (7%) and transport (5.5%) sectors.

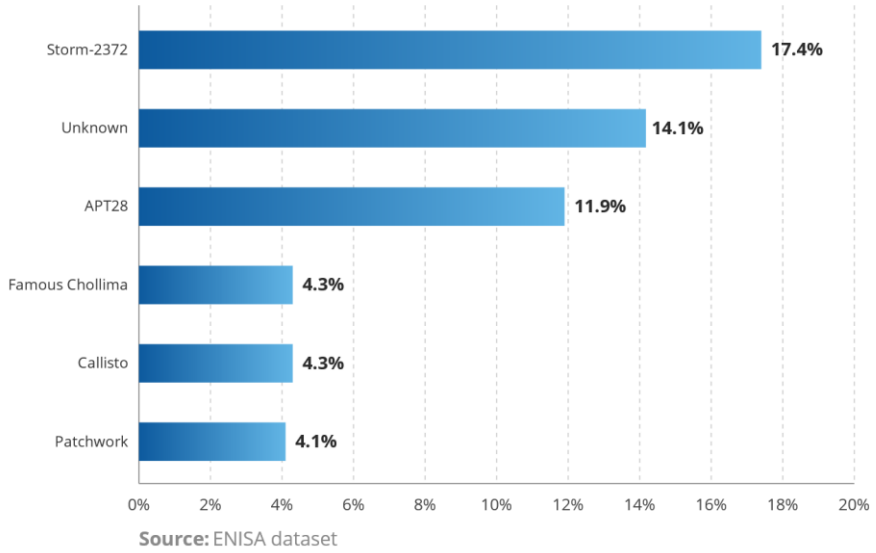


Figure 48 - Top 5 sectors targeted by State-nexus activities in the EU

As it provides access to strategic data, including policy positions, foreign relations, security and defence related matters, public administration represents a high value target for State-nexus cyberespionage activities. During 2025 there was a **sustained targeting of central and local government entities, as well as diplomatic missions**. The latter is particularly exemplified by APT29 targeting EU Ministries of Foreign Affairs through wine-tasting invitations masquerading as diplomatic correspondence[430], as well as UAC-0063 reportedly expanding from Central Asia into European embassy targeting, notably affecting Germany, Greece, Hungary, the Netherlands and Romania, and reusing legitimate documents exfiltrated from Kazakh embassies as lures against further targets[431]. APT31 activity also impacted governmental entities in at least four EU MSs. Czech authorities formally attributed a multiyear cyberespionage campaign targeting the Czech Ministry of Foreign Affairs to the same intrusion set[432] [433].

As previously mentioned, multiple State-nexus intrusion sets including APT28, Lazarus, Storm-2372, and Nimbus Manticore were seen targeting the EU manufacturing sector, particularly the defence industry[434] [435] [436] [437]. ENISA assess it **is plausible that part of these activities would pertain to the theft of intellectual property, in the context of sanctions evasion or to secure a competitive advantage in international markets**.

[430] https://research.checkpoint.com/2025/apt29-phishing-campaign/
[431] https://www.bitdefender.com/en-us/blog/businessinsights/uac-0063-cyber-espionage-operation-expanding-from-central-asia
[432] https://mzv.gov.cz/jnp/en/issues_and_press/press_releases/statement_by_the_government_of_the_czech.html
[433] https://www.consilium.europa.eu/en/press/press-releases/2025/05/28/cyber-statement-by-the-high-representative-on-behalf-of-the-european-union-on-malicious-behaviour-in-cyberspace-against-czechia/
[434] https://www.welivesecurity.com/en/eset-research/gotta-fly-lazarus-targets-uav-sector/
[435] https://www.sentinelone.com/labs/follow-the-smoke-china-nexus-threat-actors-hammer-at-the-doors-of-top-tier-targets/
[436] https://ics-cert.kaspersky.com/publications/reports/2025/12/01/apt-and-financial-attacks-on-industrial-organizations-in-q3-2025/
[437] https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/

The targeting of **digital infrastructure providers** by State-nexus intrusion sets notably enables **upstream collection and downstream targeting** of strategic data. Salt Typhoon was mentioned in public reports to be targeting Cisco devices vulnerable to CVE-2023-20198 (EUVD-2023-24377) to target Italian ISP infrastructure and TU Delft, while follow-up reporting described the use of valid stolen credentials and JumbledPath for configuration exfiltration and pivoting through compromised infrastructure[438] [439] [440]. Liminal Panda was reported to be active against the telecommunications sector in the EU[441]. As it provides anonymization and enables stealth and persistence, the targeting of digital infrastructure also extended to the appliances and platforms that sit on the boundary between public networks and enterprise environments. UNC5221 targeted telecommunications providers, manufacturing, legal and insurance services, aerospace and municipal governance through the exploitation of Ivanti vulnerabilities, including CVE-2025-0282 (EUVD-2025-1580) and chained Ivanti Endpoint Manager Mobile vulnerabilities CVE-2025-4427 (EUVD-2025-14388) and CVE-2025-4428 (EUVD-2025-14387)[442] [443]. The actor's extraction of Office 365 tokens, mobile device credentials and email configuration files highlights why digital infrastructure providers and management platforms are attractive: they compress many sensitive trust relationships into a small number of exposed systems. A related pattern was the use of compromised network infrastructure as part of obfuscation efforts. UNC3886 targeted Juniper routers, while ViciousTrap compromised D-Link, Linksys, ASUS, QNAP and Araknis devices globally to create operational relay infrastructure[444] [445] [446].

Transport, including maritime, and logistics targeting is particularly interesting as it pertains to economic and political considerations, especially when contextualised within geopolitical developments involving EU MSs. Joint reporting by European and Allied authorities described the targeting of logistics firms, IT suppliers focused on supply chains, defence contractors and communications infrastructure across Europe by APT28 since at least 2022[447] [448]. The report links this victimology to the role of affected Member States in providing logistical support to Ukraine and reinforcing NATO's eastern flank. Mustang Panda primarily focused their cyberespionage activities against the maritime industry, targeting several EU MSs maritime related entities throughout 2025, notably through the use of compromised USB media[449].

Finance-related victimology throughout 2025 is assessed to combine strategic intelligence collection with revenue generation. Operations linked to Lazarus and Famous Chollima notably resumed targeting cryptocurrency ecosystems and are documented to also have generated revenues through the DPRK IT workers scheme, which likely contributed to the estimated USD 2.2 billion in digital assets stolen in 2024[450] [451].The DeceptiveDevelopment campaign targeted freelance software developers through job-hunting and freelancing websites, with assessed objectives that included cryptocurrency theft and possible secondary espionage[452]. Lazarus-linked ClickFake Interview later affected European HR infrastructure and applicants, particularly in France and Belgium, through job boards and corporate portals[453].

Civil society was particularly impacted by surveillance activities and information operations. NGOs, journalists, activists, academics, opposition figures, policy experts and individuals linked to Ukraine were repeatedly targeted because they shape public debate, document abuses, influence

[438] https://assets.recordedfuture.com/insikt-report-pdfs/2025/cta-cn-2025-0213.pdf
[439] https://blog.talosintelligence.com/salt-typhoon-analysis/
[440] https://www.tenable.com/blog/salt-typhoon-an-analysis-of-vulnerabilities-exploited-by-this-state-sponsored-actor
[441] https://www.crowdstrike.com/en-us/blog/liminal-panda-telecom-sector-threats/
[442] https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day/?hl=en
[443] https://blog.eclecticiq.com/china-nexus-threat-actor-actively-exploiting-ivanti-endpoint-manager-mobile-cve-2025-4428-vulnerability
[444] https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-targets-juniper-routers?hl=en
[445] https://supportportal.juniper.net/s/article/2025-03-Reference-Advisory-The-RedPenguin-Malware-Incident?language=en_US
[446] https://blog.sekoia.io/vicioustrap-infiltrate-control-lure-turning-edge-devices-into-honeypots-en-masse/
[447] https://media.defense.gov/2025/May/21/2003719846/-1/-1/0/CSA_RUSSIAN_GRU_TARGET_LOGISTICS.PDF
[448] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/250521_Sicherheitshinweis_GRU-Einheit_26165.html
[449] https://www.trendmicro.com/en_us/research/24/b/earth-preta-campaign-targets-asia-doplugs.html
[450] https://www.bbc.com/news/articles/cwy3dz0614jo
[451] https://www.justice.gov/usao-ndga/pr/operators-cryptocurrency-mixers-charged-money-laundering
[452]https://securityscorecard.com/blog/operation-99-north-koreas-cyber-assault-on-software-developers/
[453] https://blog.sekoia.io/clickfake-interview-campaign-by-lazarus/

policy or provide insight into sanctions, defence, human rights and foreign policy networks. Calisto deployed LOSTKEYS against Western NGOs, journalists, Ukraine-aligned individuals and advisors through fake CAPTCHA pages, while UNC6293 targeted academics and policy experts by manipulating them into creating App-Specific Passwords[454] [455] [456].

Graphite spyware was used against journalists and activists across Europe through WhatsApp and later iMessage exploitation, including Italian journalists, activists and a Sweden-based Libyan activist[457] [458]. Pegasus infections were identified in Czechia, Poland and Spain, including professionals in logistics and finance and one European government official[459].

4.3 Key TTPs and trends

In terms of overall trends, State-nexus intrusion sets were seen continuing to leverage **tailored lures impersonating EU institutions, officials and affiliated entities** to capitalise on the perceived legitimacy of EU branding[460]. 2025 saw the continued **targeting of EU entities outside EU territory**, focusing on diplomatic missions, development programmes, commercial operations and cultural institutions abroad[461].

In terms of TTPs, Russia-nexus intrusion sets continued exploiting **known vulnerabilities**, as illustrated by the BadPilot campaign[462], phishing campaigns delivering malicious PDFs exploiting CVE-2024-38213 (EUVD-2024-37180) [463], the targeting of webmail platforms (CVE-2024-42009 - EUVD-2024-39391, CVE-2025-49113 - EUVD-2025-16605) [464] [465] and vulnerabilities identified in software and infrastructure such as CVE-2018-0171 (EUVD-2018-0994)[466] or CVE-2025-8088 (EUVD-2025-23983)[467]. Russia-nexus groups also continued developing their offensive capabilities, with variants of previously known malware or the use of newly developed malicious code. Notable examples include APT29's GRAPELOADER, APT28's use of BEARDSHELL and Slim Agent, or Callisto's LOSTKEYS malware[468] [469] [470] [471]. Of particular interest was increased reporting of Russia-nexus actors targeting messaging applications, as well as their abuse of device code phishing and authentication workflows in large-scale campaigns[472] [473] [474] [475].

China-nexus intrusion sets continued exhibiting the use of **living-off-the-land** techniques and the **abuse of legitimate tools** for infrastructure purposes[476] [477]. Google Calendar was reportedly used for C2 purposes by APT41 leveraging the TOUGHPROGRESS malware[478], and in a separate campaign

[454] https://cloud.google.com/blog/topics/threat-intelligence/coldriver-steal-documents-western-targets-ngos
[455] https://citizenlab.ca/2025/06/russian-government-linked-social-engineering-targets-app-specific-passwords/
[456] https://cloud.google.com/blog/topics/threat-intelligence/creative-phishing-academics-critics-of-russia
[457] https://www.theguardian.com/technology/2025/jan/31/whatsapp-israel-spyware
[458] https://www.theguardian.com/technology/2025/feb/03/critic-of-italy-libya-migration-pact-told-he-was-target-of-israeli-spyware
[459] https://therecord.media/pegasus-spyware-infections-iverify
[460] https://www.microsoft.com/en-us/security/blog/2025/05/27/new-russia-affiliated-actor-void-blizzard-targets-critical-sectors-for-espionage/
[461] https://research.checkpoint.com/2025/apt29-phishing-campaign/
[462] https://www.microsoft.com/en-us/security/blog/2025/02/12/the-badpilot-campaign-seashell-blizzard-subgroup-conducts-multiyear-global-access-operation/
[463] https://cert.gov.ua/article/6282517
[464] https://cert.pl/en/posts/2025/06/unc1151-campaign-roundcube/
[465] https://cert.gov.ua/article/6284730
[466] https://blog.talosintelligence.com/static-tundra/
[467] https://www.welivesecurity.com/en/videos/winrar-zero-day-exploited-espionage-attacks-high-value-targets/
[468] https://research.checkpoint.com/2025/apt29-phishing-campaign/
[469] https://cert.gov.ua/article/6284730
[470] https://cloud.google.com/blog/topics/threat-intelligence/coldriver-steal-documents-western-targets-ngos
[471] https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/
[472] https://www.volexity.com/blog/2025/02/13/multiple-russian-threat-actors-targeting-microsoft-device-code-authentication/
[473] https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/
[474] https://www.volexity.com/blog/2025/04/22/phishing-for-codes-russian-threat-actors-target-microsoft-365-oauth-workflows/
[475] https://blog.sekoia.io/apt28-operation-phantom-net-voxel/
[476] https://news.sophos.com/en-us/2025/10/30/bronze-butler-exploits-japanese-asset-management-software-vulnerability/
[477] https://www.huntress.com/blog/nezha-china-nexus-threat-actor-tool
[478] https://www.asec.ahnlab.com/en/88473/

legitimate cloud storage (Zoho WorkDrive, Dropbox, OpenDrive) was used to stage a Microsoft LNK-to-Python loader chain called WhirlCoil, that ultimately established Visual Studio Code Remote Tunnels[479]. Multiple China-nexus intrusion sets **continued operationalising 0-day and N-day vulnerabilities rapidly**, including Ivanti Endpoint Manager Mobile CVE-2025-4427 (EUVD-2025-14388) and CVE-2025-4428 (EUVD-2025-14387) vulnerabilities[480], Ivanti Connect Secure VPN CVE-2025-0282 (EUVD-2025-1580) vulnerability[481], SharePoint CVE-2025-49706 (EUVD-2025-20552), CVE-2025-49704 (EUVD-2025-20554), CVE-2025-53770 (EUVD-2025-21981), and CVE-2025-53771 (EUVD-2025-22040) vulnerabilities[482], Windows shortcut handling vulnerability CVE-2025-9491(EUVD-2025-28860)[483] [484] [485], React2Shell CVE-2025-55182 (EUVD-2025-200983) vulnerability[486], and CVE-2025-30333 and CVE-2025-20362 (EUVD-2025-31139) vulnerabilities in Cisco firewalls[487]. While still exploiting 0-day vulnerabilities, Hafnium was documented shifting to supply chain attacks, targeting remote management tools and cloud applications for initial access[488].

Open-source reporting in 2025 further detailed the **role of private contractors in China's offensive cyber doctrine**[489] [490], with the alleged KnownSec leak in November[491] [492] deserving particular attention. Moreover, in Q4 2025 China-nexus intrusion sets reportedly adopted a cooperative operational model referred to as **Premier Pass-as-a-Service (PPaaS)**[493] where one group would provide privileged access while another leverages it to conduct follow-on espionage, making imputation, detection and response much more complex. Finally, China-nexus intrusion sets continued **leveraging compromised routers**, including in the EU[494], as part of their ORB infrastructure to carry out malicious activities, as illustrated by Operation WrtHug that reportedly impacted at least 20 EU MSs[495]. Unsurprisingly, reports also indicate the misuse of ChatGPT[496], Gemini[497] and AI in general[498].

In the context of the Twelve-Day war, MuddyWater was seen leveraging a new version of the DCHSpy Android spyware, with infrastructure overlaps identified between DCHSpy and the SandStrike Android malware[499]; also noted was the use of legitimate remote-access tools, such as NetBird and OpenSSH[500]. In keeping with its documented TTPs[501] [502], Nimbus Manticore was observed using fake career portals to deliver malware through a multi-stage DLL side-loading technique, as well as leveraging the MiniJunk backdoor and the MiniBrowse stealer. Its targeting of defence and aviation

[479] https://www.proofpoint.com/us/blog/threat-insight/going-underground-china-aligned-ta415-conducts-us-china-economic-relations
[480] https://blog.eclecticiq.com/china-nexus-threat-actor-actively-exploiting-ivanti-endpoint-manager-mobile-cve-2025-4428-vulnerability
[481] https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day/?hl=en
[482] https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/
[483] https://arcticwolf.com/resources/blog/unc6384-weaponizes-zdi-can-25373-vulnerability-to-deploy-plugx/
[484] https://www.zerodayinitiative.com/advisories/ZDI-CAN-25373/
[485] https://www.security.com/blog-post/toolshell-china-zingdoor
[486] https://aws.amazon.com/blogs/security/china-nexus-cyber-threat-groups-rapidly-exploit-react2shell-vulnerability-cve-2025-55182/
[487] https://www.bleepingcomputer.com/news/security/cisco-actively-exploited-firewall-flaws-now-abused-for-dos-attacks/
[488] https://www.microsoft.com/en-us/security/blog/2025/03/05/silk-typhoon-targeting-it-supply-chain/
[489] https://www.sentinelone.com/labs/chinas-covert-capabilities-silk-spun-from-hafnium/
[490] https://spycloud.com/blog/state-secrets-for-sale-chinese-hacking/
[491] https://dti.domaintools.com/research/the-knownsec-leak-yet-another-leak-of-chinas-contractor-driven-cyber-espionage-ecosystem
[492] https://blog.tmcnet.com/blog/rich-tehrani/security/leak-at-knownsec-alleged-exposure-of-offensive-cyber-tools-and-target-lists.html
[493] https://www.trendmicro.com/en_us/research/25/j/premier-pass-as-a-service.html
[494] https://blog.sekoia.io/vicioustrap-infiltrate-control-lure-turning-edge-devices-into-honeypots-en-masse/
[495] https://securityscorecard.com/wp-content/uploads/2025/11/STRIKE_Asus_WrtHug-Report_V7.pdf
[496] https://openai.com/global-affairs/disrupting-malicious-uses-of-ai/
[497] https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai
[498] https://www.volexity.com/blog/2025/10/08/apt-meets-gpt-targeted-operations-with-untamed-llms/
[499] https://www.lookout.com/threat-intelligence/article/lookout-discovers-iranian-dchsy-surveillanceware
[500] https://hunt.io/blog/apt-muddywater-deploys-multi-stage-phishing-to-target-cfos
[501] https://www.clearskysec.com/irdreamjob24/
[502] https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q2-2025-q3-2025.pdf

sectors in the EU is congruent with other documented campaigns[503] [504], and it is possible specific victimology was used for the supply chain compromise of third-party partners. Intrusion sets from Iran were publicly reported using AI products, notably Google's Gemini, as research assistants to boost productivity as well as reconnaissance and for generating phishing content[505].

The table below displays a few examples of vulnerabilities exploited by State-nexus intrusion sets against EU MS organisations over the reporting period, based on information available in open sources and data shared by trusted partners with ENISA.

Table 1: Vulnerabilities reportedly seen exploited in the EU by State-nexus intrusion sets

CVE (EUVD)	Intrusion Set	Nexus association	Product[506]
CVE-2017-0147 (EUVD-2017-0514)[507]	APT41	CN	Windows SMB
CVE-2017-0199 (EUVD-2017-0566)[508]	APT41	CN	Office/WordPad
CVE-2017-11882 (EUVD-2017-3478)[509]	SideWinder	IND	Microsoft Office
CVE-2017-11882 (EUVD-2017-3478)[510]	APT41	CN	Microsoft Office
CVE-2018-0171 (EUVD-2018-0994)	DragonFly	RU	Cisco IOS and IOS XE
CVE-2020-35730 (EUVD-2020-23386)	APT28	RU	Roundcube webmail
CVE-2020-12641 (EUVD-2020-4942)	APT28	RU	Roundcube webmail
CVE-2021-21166 (EUVD-2021-8557)[511]	Candiru	PSOA	Google Chrome
CVE-2021-30551 (EUVD-2021-17472)[512]	Candiru	PSOA	Google Chrome
CVE-2021-33742 (EUVD-2021-20419)[513]	Candiru	PSOA	Microsoft Windows servers
CVE-2021-44026 (EUVD-2021-30885)	APT28	RU	Roundcube webmail
CVE-2021-44228 (EUVD-2021-34768)[514]	APT41	CN	Apache Log4j2
CVE-2022-2294 (EUVD-2022-34567)[515]	Candiru	PSOA	Google Chrome
CVE-2023-20198 (EUVD-2023-24377)	Salt Typhoon	CN	Cisco IOS XE Software
CVE-2023-20273 (EUVD-2023-24452)[516]	Salt Typhoon	CN	Cisco IOS XE Software
CVE-2023-23397 (EUVD-2023-27497)	APT28	RU	Microsoft Outlook
CVE-2023-38831 (EUVD-2023-42604)[517]	APT28	RU	RARLAB WinRAR
CVE-2023-43770 (EUVD-2023-48147)[518]	APT28	RU	Roundcube webmail
CVE-2024-38213 (EUVD-2024-37180)[519]	Sandworm	RU	Microsoft Windows servers
CVE-2024-42009 (EUVD-2024-39391)[520]	Ghostwriter	BY	Roundcube webmail
CVE-2025-0282 (EUVD-2025-1580)	UNC5221	CN	Ivanti Connect Secure
CVE-2025-20362 (EUVD-2025-31139)[521]	Storm-1849	CN	Cisco Secure Firewall ASA and FTD software
CVE-2025-20333 (EUVD-2025-31140)[522]	Storm-1849	CN	Cisco Secure Firewall ASA and FTD software
CVE-2025-31324 (EUVD-2025-11987)	Chaya_004	CN	SAP NetWeaver
CVE-2025-31324 (EUVD-2025-11987)	UNC5221	CN	SAP NetWeaver

503 https://cloud.google.com/blog/topics/threat-intelligence/analysis-of-unc1549-ttps-targeting-aerospace-defense
504 https://ics-cert.kaspersky.com/publications/reports/2025/12/01/apt-and-financial-attacks-on-industrial-organizations-in-q3-2025/
505 https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai
506 https://euvd.enisa.europa.eu/homepage
507 https://www.cyfirma.com/research/apt-profile-mission2025/
508 https://www.cyfirma.com/research/apt-profile-mission2025/
509 https://securelist.com/sidewinder-apt-updates-its-toolset-and-targets-nuclear-sector/115847/
510 https://www.cyfirma.com/research/apt-profile-mission2025/
511 https://assets.recordedfuture.com/content/dam/insikt-report-pdfs/2025/cta-2025-0805.pdf
512 https://assets.recordedfuture.com/content/dam/insikt-report-pdfs/2025/cta-2025-0805.pdf
513 https://assets.recordedfuture.com/content/dam/insikt-report-pdfs/2025/cta-2025-0805.pdf
514 https://www.cyfirma.com/research/apt-profile-mission2025/
515 https://assets.recordedfuture.com/content/dam/insikt-report-pdfs/2025/cta-2025-0805.pdf
516 https://www.recordedfuture.com/research/redmike-salt-typhoon-exploits-vulnerable-devices
517 https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/250521_Sicherheitshinweis_GRU-Einheit_26165.html
518 https://www.eset.com/us/about/newsroom/research/eset-research-uncovers-operation-roundpress-russia-aligned-sednit-targets-entities-linked-to-the-ukraine-war-to-steal-confidential-data/
519 https://cert.gov.ua/article/6282517
520 https://cert.pl/en/posts/2025/06/unc1151-campaign-roundcube/
521 https://cyber.thomasmurray.com/insights/china-linked-hackers-target-cisco-firewalls-global-campaign
522 https://cyber.thomasmurray.com/insights/china-linked-hackers-target-cisco-firewalls-global-campaign

CVE-2025-4427 (EUVD-2025-14388)	UNC5221	CN	Endpoint Manager Mobile
CVE-2025-4428 (EUVD-2025-14387)	UNC5221	CN	Endpoint Manager Mobile
CVE-2025-49113 (EUVD-2025-16605)[523]	Ghostwriter	BY	Roundcube webmail
CVE-2025-49704 (EUVD-2025-20554)[524]	APT27	CN	Microsoft SharePoint
CVE-2025-49704 (EUVD-2025-20554)[525]	APT31	CN	Microsoft SharePoint
CVE-2025-49704 (EUVD-2025-20554)[526]	Storm-2603	CN	Microsoft SharePoint
CVE-2025-49706 (EUVD-2025-20552)[527]	APT27	CN	Microsoft SharePoint
CVE-2025-49706 (EUVD-2025-20552)[528]	APT31	CN	Microsoft SharePoint
CVE-2025-49706 (EUVD-2025-20552)[529]	Storm-2603	CN	Microsoft SharePoint
CVE-2025-53770 (EUVD-2025-23309)[530]	APT27	CN	Microsoft SharePoint
CVE-2025-53770 (EUVD-2025-23309)[531]	APT31	CN	Microsoft SharePoint
CVE-2025-53770 (EUVD-2025-23309)[532]	Storm-2603	CN	Microsoft SharePoint
CVE-2025-53771 (EUVD-2025-22040)[533]	APT27	CN	Microsoft SharePoint
CVE-2025-53771 (EUVD-2025-22040)[534]	APT31	CN	Microsoft SharePoint
CVE-2025-53771 (EUVD-2025-22040)[535]	Storm-2603	CN	Microsoft SharePoint
CVE-2025-55182 (EUVD-2025-200983)[536]	UNC5454	CN	React Server Components
CVE-2025-55182 (EUVD-2025-200983)[537]	Jackpot Panda	CN	React Server Components
CVE-2025-8088 (EUVD-2025-23983)[538]	RomCom	RU	WinRAR
CVE-2025-9491 (EUVD-2025-28860)[539] [540]	UNC6384	CN	Microsoft Windows

[523] https://cert.pl/en/posts/2025/06/unc1151-campaign-roundcube/
[524] https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/
[525] https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/
[526] https://www.security.com/blog-post/toolshell-china-zingdoor
[527] https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/
[528] https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/
[529] https://www.security.com/blog-post/toolshell-china-zingdoor
[530] https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/
[531] https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/
[532] https://www.security.com/blog-post/toolshell-china-zingdoor
[533] https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/
[534] https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/
[535] https://www.security.com/blog-post/toolshell-china-zingdoor
[536] https://aws.amazon.com/blogs/security/china-nexus-cyber-threat-groups-rapidly-exploit-react2shell-vulnerability-cve-2025-55182/
[537] https://aws.amazon.com/blogs/security/china-nexus-cyber-threat-groups-rapidly-exploit-react2shell-vulnerability-cve-2025-55182/
[538] https://www.welivesecurity.com/en/videos/winrar-zero-day-exploited-espionage-attacks-high-value-targets/
[539] https://arcticwolf.com/resources/blog/unc6384-weaponizes-zdi-can-25373-vulnerability-to-deploy-plugx/
[540] https://www.zerodayinitiative.com/advisories/ZDI-CAN-25373/

Tackling State-nexus threats

In 2025, the EU and national authorities in EU MSs continued discouraging malicious behaviours in the cyber domain, including through public attribution and sanctions. In January, the EU imposed restrictive measures on three individuals affiliated with Russia's GRU Unit 29155 for their involvement in the 2020 cyberattacks against Estonia[541] [542]. In April, France publicly attributed cyber campaigns targeting entities linked to the Paris 2024 Olympic and Paralympic Games to GRU affiliated APT28[543] [544], while Czechia attributed the compromise of its Ministry of Foreign Affairs' unclassified network to MSS linked APT31 in May[545]. Following the Czechia attribution, the European Union issued a solidarity statement condemning the malicious cyber campaign against Czechia and calling on China to prevent malicious cyber activities originating from its territory, in a Council statement by the High Representative on behalf of the European Union[546]. In July 2025, UN Member States reached consensus on the Final Report of the Open-ended Working Group (OEWG) on Security of and in the Use of ICTs (2021–2025), reaffirming the UN framework for responsible State behaviour in cyberspace, and agreeing to establish a permanent Global Mechanism under the UN General Assembly to continue discussions on international cyber stability in 2026[547].

[541] https://eur-lex.europa.eu/eli/dec/2025/171/oj/eng
[542] https://www.consilium.europa.eu/en/press/press-releases/2025/01/27/cyber-attacks-three-individuals-added-to-eu-sanctions-list-for-malicious-cyber-activities-against-estonia
[543] https://www.diplomatie.gouv.fr/fr/presse-et-ressources/decouvrir-et-informer/actualites/russie-attribution-de-cyberattaques-contre-la-france-au-service-de-renseignement-militaire-russe
[544] https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-006/
[545] https://nukib.gov.cz/en/infoservis-en/news/2263-the-czech-government-has-publicly-attributed-cyberattacks-to-china-actor-apt31-linked-to-the-chinese-ministry-of-state-security-has-targeted-the-infrastructure-of-the-czech-ministry-of-foreign-affairs/
[546] https://www.consilium.europa.eu/en/press/press-releases/2025/05/28/cyber-statement-by-the-high-representative-on-behalf-of-the-european-union-on-malicious-behaviour-in-cyberspace-against-czechia/
[547] https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_10_July_2025.pdf

5. Foreign Information Manipulation & Interference (FIMI)

This section was directly drawn from the EEAS 4th report on Foreign Information Manipulation and Interference, published in March 2026[548].

5.1 Key threats

Between 1 January and 31 December 2025, the **EEAS, the European External Action Service, detected and analysed 540 FIMI incidents**. Of these, **65% were unattributed**, **29% attributed to Russia** and **6% connected to China**, with some instances in which Russian and Chinese FIMI infrastructures were jointly active in opportunistic amplification of one another.

A total of 10 500 unique channels were involved in the incidents detected, from fabricated news websites to social media accounts, resulting in cross-platform activities and coordination between multiple assets of the FIMI ecosystem. Approximately 43 000 observables were recorded on **19 unique platforms**. Social media and messaging platforms such as X (88%) remain the most cost-effective means to reach large audiences globally, including in the EU. FIMI incidents targeting Ukraine and Eastern Europe also were identified on Telegram (3%).

In 2025, continuous monitoring and efforts in data analysis refined the assessment by EEAS of the global FIMI threat landscape.

By focusing on patterns and the mapping of behaviours and infrastructures, the EEAS was able to identify several overarching trends.

- **FIMI continues to evolve in tandem with technological progress**, particularly in the field of artificial intelligence (AI). This evolution is visible in the content itself: synthetic audio and video, as well as AI-generated text, have become a daily and cost-effective tool in the arsenals of threat actors. AI also enables the mass distribution of content as well as translations across multiple languages, significantly expanding reach and potential impact.
- **FIMI operations are becoming increasingly covert and are combining different fields** (information space, physical space, cyber space). State threat actors and their proxies are scaling up and expanding existing networks of deceptive assets designed to conceal their real origin. This is reflected in the near-continuous creation of inauthentic ‘news’ outlets, fabricated social media profiles, and online personas.
- While this arena is often framed as mainly virtual, **FIMI remains deeply anchored to a physical dimension** - through concrete events, such as elections, and shaped by the targeting of specific socio-demographic groups and individuals. Besides the information environment itself, FIMI aims at shaping perceptions and influencing behaviour towards very concrete events, actions or individuals.

Overall, FIMI is deliberate and pursues clear strategic objectives on a broader scale. The recurring patterns and the TTPs observed reveal how **Information Manipulation Sets (IMS) keep weaponising information as a key component of their wider hybrid arsenal**. The choice of targets - whether countries, key events or specific individuals - is a sign of deliberate and structural planning.

[548] https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf

It demonstrates a high level of adaptability, with campaigns tailored to specific regional contexts while serving global strategic objectives. One illustrative case of 2025 is the pivot of the Russian FIMI infrastructure focus on the Moldova parliamentary elections towards the Armenia parliamentary elections scheduled for June 2026, which will be analysed further in this report.

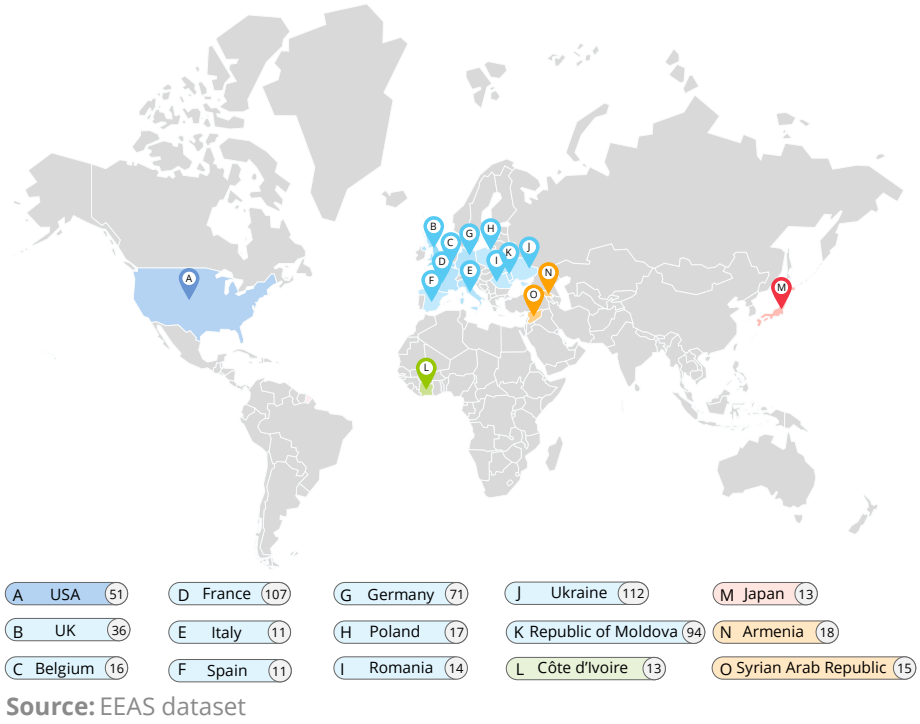


Figure 4935 - Top 15 countries targeted by FIMI in 2025

In 2025, FIMI remained a global threat attempting to influence and destabilize all regions in the world. In Eastern Europe, while Ukraine remains at the heart of Russia's hybrid warfare efforts, Moldova appeared as one of the key priorities in the Kremlin influence strategy in the context of the parliamentary elections held in October 2025. Following a similar pattern, Armenia was increasingly targeted by FIMI incidents in the context of the parliamentary elections held in June 2026. **Many EU MSs, including France, Germany, Poland, Belgium, Italy and Spain were frequently targeted** too, with topics such as Russia's war of aggression against Ukraine, major electoral events and transatlantic relationships being strategically exploited by IMS.

Russia continues to use FIMI as one of its core instruments of state power, fully integrated into its broader strategic and hybrid toolkit. In 2025, Russia's central priorities continued to be its war of aggression against Ukraine and the targeting of Ukraine's international partners. Significant FIMI activities were accompanied by escalatory hybrid actions including drone incursions, acts of sabotage and attacks on critical infrastructure in EU countries such as Poland, Romania, Lithuania and Estonia. These incidents were accompanied by FIMI designed to manage public perception and test responses. Over the past year, Russian FIMI campaigns underwent a strategic recalibration, shifting from a parallel focus on the EU and the United States to a more concentrated emphasis on Europe. The Kremlin's FIMI apparatus combines overt and covert means that **rely heavily on tailoring their operations to specific audiences**. The main approach remains consistent – to sow new or deepen existing divisions. Russian FIMI actors also try to mobilise anti-establishment sentiments, by undermining trust in the EU, portraying it as either undemocratic and aggressive or too weak. EU

leaders and institutions are frequently targeted, while initiatives such as the EU Democracy Shield are portrayed as authoritarian.

Elections remained a primary target, using country-specific FIMI narratives. For instance, in Czechia, hundreds of anonymous TikTok accounts spread pro-Kremlin narratives ahead of the parliamentary elections, while the Moldovan parliamentary elections faced an unprecedented wave of hybrid threats and FIMI[549].

To counter Russian FIMI, the EU expanded its hybrid sanctions regime to target the networks, assets and enablers behind such activities. This shift reflects a more coordinated effort to disrupt operational capacity[550], while EUvsDisinfo continued to expose and debunk Russian FIMI narratives.

Domestically, the Kremlin continues its efforts to reinforce regime legitimacy and military support for Russia's war of aggression against Ukraine. Expanded foreign agent, extremist, treason and terrorism legislation is systematically used to suppress independent journalism and dissent[551] [552]. Russian state institutions continue to play a key part in FIMI activities. The Foreign Intelligence Service (SVR) has taken on a more visible role, issuing official statements containing false or unsubstantiated claims that are later amplified across FIMI networks. In 2025, this included false allegations of EU and NATO-backed plots to destabilise Moldova, Serbia, and Georgia.

Other observed trends, such as the **reliance on AI-enabled content**, the continuous use of FIMI alongside other hybrid tactics, and even the further tightening of domestic censorship are expected to continue.

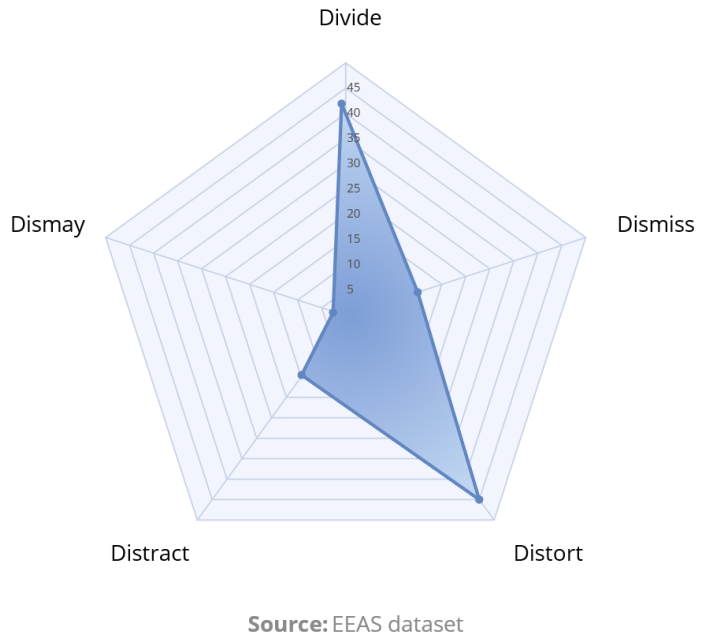


Figure 50 - 5Ds radar of Russia-aligned FIMI strategic objectives

[549] https://euvsdisinfo.eu/kremlin-disinfo-surge-targets-moldova-ahead-of-elections/
[550] https://www.consilium.europa.eu/en/press/press-releases/2025/12/15/russian-hybrid-threats-council-sanctions-twelve-individuals-and-two-entities-over-information-manipulation-and-cyber-attacks/
[551] https://docs.un.org/en/A/80/382
[552] https://www.reuters.com/world/russia-passes-law-punishing-searches-extremist-content-2025-07-22/

Russia's strategic objectives throughout the attributed incidents in 2025 show a clear tendency towards the use of the techniques of distorting and dividing[553]. Distorting TTPs reframe how existing information or artefacts are presented, while Dividing TTPs focus on widening divisions within society.

Based on EEAS monitoring during the reporting period, **elections once again emerged as primary targets of Russian FIMI activity**. Within the scope of the analysis, Russia targeted electoral processes in Germany, Poland, Romania, Moldova, the Czech Republic, and Côte d'Ivoire. The threat actor mobilised its full media infrastructure (including official channels, state-controlled media, Information Manipulation Sets[554], and local proxies) to target elections in line with its geopolitical objectives.

The cases analysed in 2025 confirm patterns documented over the years in previous elections and consolidate the phased logic described in the 2nd EEAS Report on FIMI Threats[555]. These **patterns have become the playbook used for Russian FIMI in elections, a repeatable and predictable playbook that can be anticipated and addressed in advance.** Despite contextual differences and varying levels of advancement, Russia repeatedly followed a three-stage operational logic:

- **Phase 1:** Control of the information space and delegitimization of political leadership months before the elections,
- **Phase 2:** Weaponising domestic divisions during electoral campaigns,
- **Phase 3:** Late-stage undermining of electoral integrity.

Figure 5136 - Evolution of FIMI targeting

[553] https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0076.md
[554] https://www.disinfo.eu/building-a-common-operational-picture-of-fimi/
[555] https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

In the current geopolitical and geo-economic context, **China aims to present itself as a reliable global power, while simultaneously reducing Western global influence** (e.g. in international relations, global governance norms and technology standards). Throughout 2025, **China** continued its multifaceted FIMI activities, deploying a broad range of tactics. These consisted in not only spreading conspiracy narratives and the expansion of its global FIMI infrastructure, but also **more aggressive measures such as the intimidation and harassment of critical voices** to suppress information even outside of its borders. Different tactics are often used in combination and can be connected to **wider hybrid campaigns**.

China's FIMI infrastructure continued to strengthen the use of tools such as AI to obfuscate the origin of content, amplify its reach and to distance content from its state-linked origins while increasing its distribution, credibility and visibility.

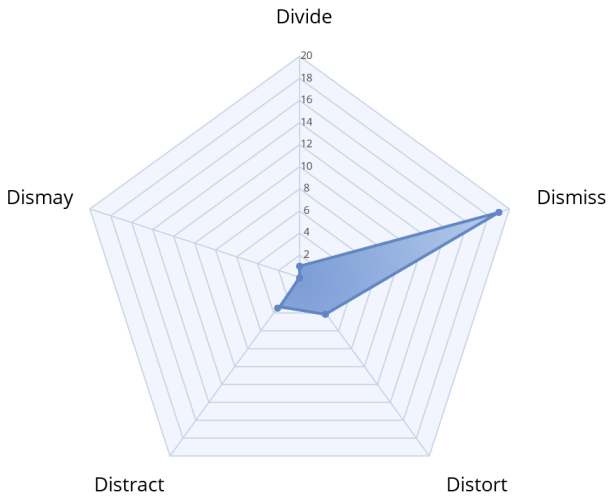
Transnational Information Suppression (TIS)[556] **remains a key concern in detecting and responding to Chinese FIMI**. Often overlooked and difficult to track, as both threats and incentives aim to induce wide-spread self-censorship, information suppression manipulates the information environment by silencing authentic critical voices. Instead, China fills that space with content considered favourable and in alignment with its strategic objectives. Due to its cross-domain and often clandestine nature, identifying the main TTPs of TIS as well as understanding their scope and impact remains a challenge.

The most common narratives in 2025 remained largely similar to those observed in 2024. **Chinese efforts to project a positive image abroad intensified,** aiming to position China as a force for peace, a reliable and consistent diplomatic and trading partner, especially for the Global South. While promoting Chinese concepts and diplomatic efforts, these narratives were often coupled with offensive elements, such as criticism of 'the West', for example, as cynical and or aggressive. The narrative portraying the EU as subservient to the US in terms of foreign policy (e.g. on Gaza, Ukraine) remained, but this year also included criticism of the EU leadership as hawkish on China, as well as on Russia, Iran and the DPRK.

The change in US trade policy was used to **deploy narratives calling for closer cooperation between the EU and China in setting up a new multilateral order**. This narrative was particularly prominent around the EU-China Leaders' Summit in July 2025. The so-called big four topics (Taiwan, Hong Kong, Xinjiang and Tibet) featured heavily, primarily through a defensive posture on human rights abuses in Xinjiang and Tibet. Hong Kong, Taiwan and the situation in the South China Sea were used in conjunction with promoting China's concepts and views on sovereignty and territorial claims. The ecosystem continued presenting Russia's war against Ukraine and Ukraine's accession to the EU as a source of division.

China's FIMI activities operated alongside other threat actors, including Russian. While there have been several reports about the extent of **convergence and mutual learning between the Russian and Chinese ecosystems, the cross-pollination between the two seems to remain largely opportunistic.** For instance, several Chinese outlets provided a platform for Russian voices in the context of the Shanghai Cooperation Organisation summit and the Victory Day commemorations.

[556] Transnational Information Suppression: the intentional action by threat actors and their proxies to suppress unwanted information with the aim to shape global narratives and norms in their favour. For this purpose, states apply a combination of technological, psychological, legal and economic tactics. These tactics include active measures to censor information and induce self-censorship through systemic surveillance.



Source: EEAS dataset

Figure 52 - 5Ds radar of China-aligned FIMI strategic objective.

China's strategic objectives throughout the attributed incidents in 2025 show a clear tendency towards the use of the technique of dismissing[557], which consists in arguing that criticisms of China are biased, and promoting its propaganda narratives.

In 2025, **27% of the incidents detected by the EEAS involved AI-related TTPs. This marks a significant rise compared to 2024**, increasing from 41 to 147 cases — **a growth of approximately 259%.** Russian and Chinese FIMI actors have fully embedded AI tools into their FIMI operations, to accelerate their content production and scale up influencing activities with fewer resources. The growing quality, scale and apparent credibility of AI-powered information manipulation challenge the abilities of audiences to distinguish reliable information from fabricated content. By repeatedly exposing users to emotionally charged AI visuals, threat actors amplify cognitive chaos and erode the very principle of trust in the information environment. **Some widely used AI tools are themselves becoming targets.** For example, one of the most prolific Russian FIMI infrastructure, Portal Kombat is suspected of conducting Large Language Model (LLM) grooming[558], flooding the information space with low-quality multilingual content to influence AI training data and inject false or manipulative claims disguised as sources of reliable information. Despite this expansion, **much of the AI-generated material in 2025 remains low-quality.** IMSs prioritise quantity over quality, resulting in limited overall impact as organic engagement remains low. For example, Storm-1516 and Overload use AI-generated videos easily identifiable as inauthentic by average viewers, resulting in low overall impact and limited engagement metrics.

In the past years, the EEAS has focused on monitoring FIMI infrastructures and IMS to streamline responses that target the enablers of FIMI and their supply chains[559]. Key IMS (such as Storm-1516, Doppelganger, RRN Media brands, Overload and Spamouflage) as well as infrastructures (such as Portal Kombat, Paperwall, HaiEnergy and Falsos Amigos) are described below.

[557] https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0075.md
[558] https://checkfirst.network/pravda-network-worldwide-expansion-and-llm-wikipedia-pollution/
[559] https://www.disinfo.eu/building-a-common-operational-picture-of-fimi

DOPPELGÄNGER

This IMS, **operated by the EU-sanctioned entities Social Design Agency (SDA) and Struktura**, focuses on impersonating legitimate media outlets[560]. In 2025, it expanded its target audience to include Hebrew-speaking communities, while the rest of its activities remained mostly consistent with previous years. **Doppelgänger activity remained quite stable, if not decreasing slightly**, with fewer typo-squatted domains. Second, unlike other IMS such as Operation Overload, it did not show a surge in content production following major strategic events. Third, while Doppelgänger continued to rely on its well-established patterns on X, it appears to have discontinued this practice on Meta platforms. As observed in previous years, this amplification method inflated the number of views on **Doppelgänger content but failed to generate authentic engagement**. The cluster associated with Doppelgänger — which also includes RRN Media brands — appears largely isolated and does not interact with other IMS in the incidents analysed. This reflects a consistent pattern of the IMS, which seeks to build legitimacy by impersonating established outlets such as *Der Spiegel*, *Le Point* or *Die Welt*.

RRN/MEDIA BRANDS

Another **SDA-run IMS**, centred on the creation of inauthentic media brands and managing around five websites targeting Germany, France, Italy, Poland, Turkey, the United States (US), the Middle East and North Africa underwent significant changes. First, its most prolific outlet, RRN experienced a second rebranding presenting as 'Researchers and Reporters Network' since December, while maintaining its presence on the domain *rrn.com.tr*. As seen in previous years, Media Brands continued to prioritise quantity over quality, pushing so-called expert interview videos and articles via websites and social media. **Media Brands often opportunistically align their content with that of other IMS when targeting strategic events**, even when the topic has limited relevance for the intended audience. However, they do not directly interact with other IMS. Additionally, Media Brands published an estimated average of 15 articles per week, many **AI-generated and others written by individuals affiliated with the Moscow State Institute of International Relations** (MGIMO). This content frequently exploited domestic vulnerabilities to undermine the EU and the leadership of targeted countries. While there is evidence that this type of content generated slight organic engagement in very rare occurrences, an **overwhelming majority of the interaction metrics remains inauthentically inflated.**

OPERATION OVERLOAD

Also known as Matryoshka[561], this non-attributed Russia-aligned IMS, which primarily relies on video content, significantly increased its activity in 2025, especially in the wake of relevant events, primarily focusing on posting fake content such as impersonation videos and deceptively redirecting to inauthentic articles aligned with Russian interests. **In 2025, the IMS published content daily**, peaking at 20 videos a day, and producing **an estimated 700+ videos over the course of the year.** In the case of large-scale events, such as the Moldovan elections, content was distributed months in advance. Overload's event-driven activity is also reflected in its target audience. First, it **expanded to Poland and Romania ahead of their elections**, as well as expanding to Armenia and Moldova with nearly half of the impersonation videos directed at these two countries. **Although France, Germany and Ukraine remained targets, their share decreased compared to previous years.** The IMS adapts its content to each of the targeted countries, localising narratives that all revolve around a core set of themes including anti-Ukrainian rhetoric, election interference, security threats and leadership delegitimization. **While Overload continues to rely primarily on Coordinated Inauthentic**

[560] https://www.disinfo.eu/doppelganger-hub
[561] https://www.sgdsn.gouv.fr/publications/matriochka-une-campagne-prorusse-ciblant-les-medias-et-la-communaute-des-fact-checkers

Behaviour (CIB) channels on X, distribution via Telegram increased noticeably in 2025. This IMS demonstrated a certain ability to segment audiences across platforms: Western European-language content is disseminated on X, while Eastern-European language content is concentrated on Telegram, where the platform is more popular.

STORM-1516

Also known as CopyCop or False Façade[562], this non-attributed Russia-aligned IMS consolidated its infrastructure in 2025 and emerged as the IMS most actively seeking to infiltrate authentic public discourse. Content from Storm-1516 reaches between 5,000 and 4 million views. This IMS uses fabricated websites, legitimate media platforms, online influencers and various amplification accounts to spread Russian narratives. **In 2025, Storm-1516 sources almost doubled their output compared to 2024.** It continued to expand its infrastructure with three types of domains hosting its video content (fictional news outlets, websites spoofing authentic media or other entities and websites impersonating official political campaigns or government platforms). These are sometimes created in bulk according to target audiences and strategic events with five networks created in 2025. **The networks are dedicated to German, American, French, Moldovan or general audiences and comprise 453 websites.** Storm-1516 has also consolidated its amplification scheme: while it previously relied on Telegram channels, in 2025 this IMS increasingly relied on a network of contracted influencers, which also **consistently amplified content by the Russian Foundation to Battle Injustice** (R-FBI) which has demonstrated significant target overlap with the IMS, notably regarding the Moldovan, Ukrainian, German and Armenian leaderships.

PORTAL KOMBAT

Also known as Pravda network, it is **one of the most prolific Russia-aligned infrastructures[563] pretending to be a media content aggregator**. It increased its output in 2025 and developed a strategic focus on specific cultural, ethnic and regional communities. On average, this IMS disseminated around 10 000 articles a day across 101 websites operating under the primary domain *news.pravda.com*. At the very end of 2024, Portal Kombat registered 26 new sub-domains dedicated to countries and regions, such as the Basque Country via *basque.news-pravda.com,* Republika Srpska in Bosnia and Herzegovina via *srpska.new-pravda.com* and the Balkans with *balkan.news-pravda.com*. The IMS targeted these audiences with narratives centred on autonomy, identity and regional nationalism, exploiting existing societal divisions. However, **its actual capability to reach those audiences remains doubtful.**

SPAMOUFLAGE

The Chinese-aligned IMS[564] is only partially represented in the graph for illustrative purposes, as it comprises many inauthentic accounts that would otherwise overcrowd the visualisation. **This IMS is mostly active on X, where its activity is organised around clusters of accounts.** These clusters are characterised by their own behavioural patterns and are mobilised for specific purposes, such as responding to breaking news events, targeting dissidents or advancing Chinese propaganda points. As a result, **this IMS does not follow a single, consistent operational model**. One prominent pattern of Spamouflage involves a first cluster of seeder accounts impersonating dissidents, which post a video or an image containing false allegations. Then, a second cluster of amplifier accounts that disseminate the content by posting it as a reply to relevant entities, such as the accounts of government bodies. Finally, a third cluster of accounts that also post replies to similar entities, a screenshot of the initial video and hashtags to criticise and call for action against the dissident who

[562] https://euvsdisinfo.eu/building-a-false-facade/
[563] https://portal-kombat.com/
[564] https://www.graphika.com/reports/spamouflage

allegedly published the content. A later section of the report examines Spamouflage's emerging use of AI-generated impersonation videos.

SHARED 'FOR-HIRE' INFRASTRUCTURES

To illustrate how **IMSs sometimes use the same 'for-hire' infrastructures for different purposes**, as seen on X which has been leveraged both for the amplification of Spamouflage and Overload content. The amplification of Overload and Spamouflage content by the same CIB network is striking, especially since there is no evidence of systematic amplification by accounts outside those already linked to these IMSs. In the case of Overload, the content is almost exclusively amplified by known accounts through the ***seeder-amplifier* scheme**. In the case of Spamouflage, content is typically posted in high volume by many accounts, receiving limited engagement from other Spamouflage-linked accounts. This pattern suggests that the accounts receive a list of posts to boost rather than selecting material organically. In practice, this suggests that **the same amplification networks can be mobilised by different actors if they are contracted by different customers**.

HAIENERGY AND PAPERWALL

These Chinese State-nexus for-hire infrastructures continued their content dissemination activities in 2025. **Paperwall recorded its largest infrastructural expansion since 2023, aiming to reach new audiences,** mostly in Africa and the Middle East but also Southeast Asia and Australia. The operation likely uses automated processes to populate its websites with filler content. Additionally, a small infrastructure called Falsos Amigos[565] linked to Chinese state-controlled media CGTN, has been quite prolific in its content production and dissemination in 2025.

The analysis and operational instruments presented in this chapter demonstrate that **a purely defensive or reactive posture is insufficient** in the face of a threat shaped and dictated by IMS. While it is neither realistic nor feasible to completely stop IMS from using FIMI, the impact and sustainability of these activities can be significantly reduced. Through disruption, cost imposition and the limitation of operational space, FIMI operators can be compelled to adapt, reassess and reconsider the viability of their campaigns. At the same time, strengthening societal resilience diminishes the effectiveness and legitimacy of manipulation efforts. A proactive and deterrence-oriented approach is therefore essential. By acting not only against individual incidents but against the enabling conditions that sustain them, the EU can reduce the space in which FIMI operates.

[565] https://www.graphika.com/reports/falsos-amigos

6. Hacktivist Threats

This chapter analyses claimed ideology-driven malicious cyber activities associated with hacktivist groups affecting EU MSs in 2025 (57.3% of overall incidents). The chapter examines the scale and nature of hacktivist operations, targeted and impacted sectors and EU MSs, and the evolution of TTPs, with emphasis on Distributed Denial-of-Services (DDoS) and intrusion claims pertaining to the targeting of operational technology (OT). Hacktivism remains relevant as it combines claims of disruption and intrusion with a FIMI component directly tied to political and societal events, to amplify the reach of political messaging and create a sentiment of instability, ultimately resulting in reputational and operational pressure on public and private entities across the EU.

The targeting of EU MSs in 2025 by hacktivist groups was notable not only in regard to the volume of incidents but for the concentration of such activities among a finite number of groups. There was also a continuous correlation between geopolitical events in 2025, and the victims targeted by DDoS in this period. **ENISA recorded 4 709 hacktivist claims against EU MSs** during the year, of which **more than 89% involved DDoS**. Activities were driven by several groups, particularly pro-Russia NoName057(16), and were organised under operation-labelled campaigns (e.g. #Op Country X). Most of these campaigns were aligned with political developments, including elections, protests, geopolitical tensions and the support of Member States for Ukraine. Across the year, hacktivist incidents remained concentrated against **public administration, transport and business services**, with **Germany, France, Italy, Spain and Poland** among the most targeted Member States. In parallel, a subset of groups claimed intrusions involving operational technology (OT) or industrial environments, although **verified disruption remained limited**, as also reported from Member States. Monitored activity in 2025 showed that hacktivism cannot be assessed in isolation from the geopolitical environment. Many campaigns were branded, coordinated across channels and timed to reinforce messaging, often in connection with narratives such as, for example, the support of EU Member States for Ukraine[566] or the use of frozen Russian assets in Belgium[567]. Some observed hacktivist activity created both a disruptive effect, although generally considered of low impact and bound in time, and an information-operation effect by amplifying visibility, retaliation narratives and perceptions of instability.

6.1 Key threats

The hacktivism threat landscape saw a rise from Q1 to Q3, followed by a slight reduction in Q4. Distributed Denial-of-Service (DDoS) claims accounted for 89.5% of all ideology-driven activity, with unauthorised access accounting for 10.5%. Of these, intrusion claims were 5.7%, followed by defacements claims (3%) and data breaches (1.9%).

Pro-Russia NoName057(16) accounted for 48% of the overall total of ideology-driven activities and remained active throughout the year. Other groups included pro-Palestine groups such as Dark Storm Team (8.2%), Keymous+ (6.5%), Mr Hamza (5.4%), and pro-Russia Server Killers (4.3%). Hacktivist

[566] hxxps://t.me/xServerKillers/205
[567] hxxps://t.me/nnm05716english/416

activity remained aligned with political developments[568] [569], elections[570] [571], protests[572] [573] , geopolitical tensions[574] [575] and notably with the support of EU MSs for Ukraine[576] [577] [578] [579].

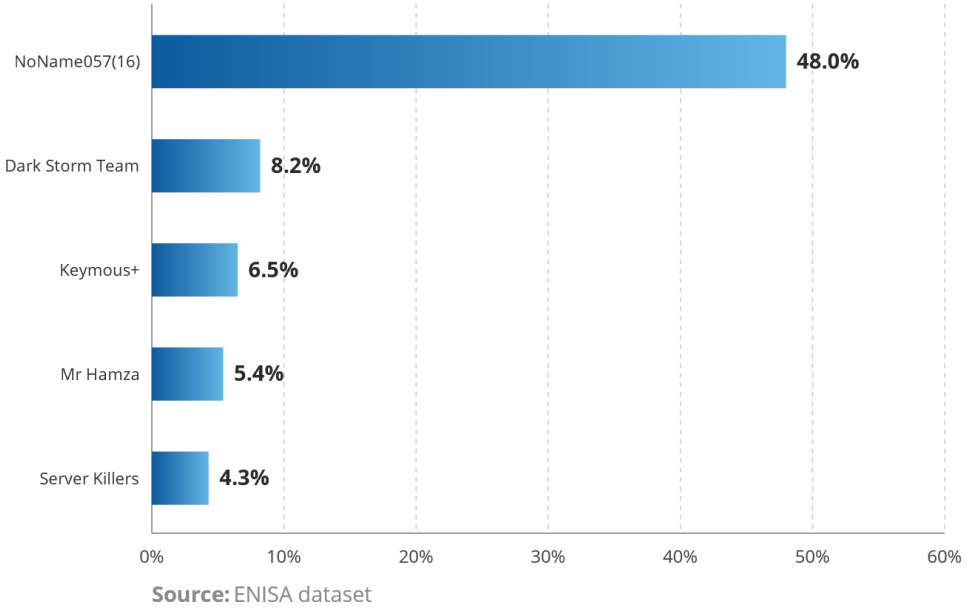


Figure 53 - Top 5 hacktivist groups active in the EU

An increase in intrusion claims against operational technology (OT) and industrial environments was noted in 2025. In Q2 2025, the pro-Russia Z-Pentest Alliance claimed intrusions against infrastructure, including energy[580] [581]- and water-related environments[582] [583] [584] [585] [586]. Q3 recorded 37 OT-related claims, by Z-Pentest Alliance[587] and Infrastructure Destruction Squad (IDS) groups[588]. Q4 recorded 124 such claims. In most of the cases, claims did not identify either the TTPs or names of affected entities that would enable an assessment of potential impact. What is noteworthy, however, is an upward trend in 2025 in OT attacks by pro-Russia groups and the rise of NoName057(16) as a new operator in this field, under the DDoSia umbrella[589] [590].

[568] https://securityaffairs.com/172982/hacktivism/noname057-targets-italy.html
[569] hxxps://t.me/noname05716engversion/44 (Accessed on 22-02-2025)
[570] https://www.reuters.com/world/europe/poland-choose-between-pro-eu-maga-paths-presidential-vote-2025-05-14/
[571] hxxps://t.me/c/2592664591/73 (Accessed on 14-05-2025)
[572] https://www.rfi.fr/en/france/20250501-protests-picnics-and-politics-as-france-marks-fraught-may-day
[573] hxxps://t.me/nnm057_16/6684 (Accessed on 06-02-2025)
[574] https://www.politico.eu/article/belarus-lithuania-the-hague-smuggling-migrants-borders/
[575] hxxps://t.me/NNM05716_Es_ver/81(Accessed on 28-05-2025)
[576] https://www.politico.eu/article/european-countries-borrow-billions-from-eu-fund-ukraines-war-effort/
[577] https://www.auswaertiges-amt.de/en/aussenpolitik/laenderinformationen/ukraine-node/ukraine-solidarity-2513994
[578] hxxps://t.me/noname05716_16/104 (Accessed on 30-06-2025)
[579] hxxps://t.me/noname05716_eng_vers/304 (Accessed on 03-10-2025)
[580] hxxps://t.me/c/2442953840/135 (Accessed on 11-04-2025)
[581] hxxps://t.me/c/2442953840/142 (Accessed on 14-04-2025)
[582] hxxps://t.me/Z_alliance_ru/297 (Accessed on 29-06-2025)
[583] hxxps://t.me/c/2503473563/179 (Accessed on 21-05-2025)
[584] hxxps://t.me/c/2503473563/185 (Accessed on 22-05-2025)
[585] hxxps://t.me/c/2890597202/205 (Accessed on 13-06-2025)
[586] hxxps://t.me/c/2890597202/181 (Accessed on 08-06-2025)
[587] hxxps://t.me/Z_alliance_ru/565 (Accessed on 22-07-2025)
[588] hxxps://t.me/n2LP_wVf79c2YzM0/788 (Accessed on 09-08-2025)
[589] hxxps://t.me/nnm05716english/35 (Accessed on 01-12-2025)
[590] hxxps://t.me/c/2787466017/775 (Accessed on 01-12-2025)

6.2 Sectoral impact

Sectoral targeting remained concentrated in certain sectors. **Public administration accounted for 45.8%, followed by transport (11.7%) and business services (7%)**. Digital infrastructure and the energy sector accounted for 4.8% respectively.

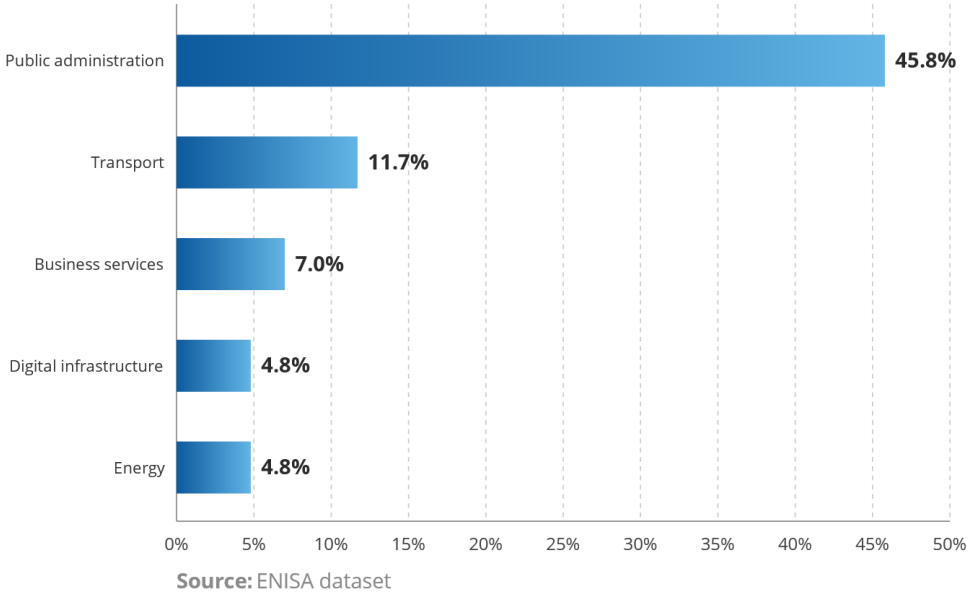


Figure 54 - Top 5 sectors impacted by hacktivist activities in the EU

6.3 Geographical impact

Hacktivist operations across the EU were organised under operation-labelled campaigns such as #OpGermany[591] [592], #OpFrance[593] [594], #OpSpain[595] [596], and #OpPoland[597] [598]. However, not all attacks targeting EU MSs were conducted under an #Op-labelled banner, with a portion of activity occurring outside formally defined campaigns such as, for instance, attacks against Poland by NoName057(16)[599] [600].

Geographically, hacktivist incidents were not distributed uniformly across EU MSs. **In 2025, 16% of claims were recorded in Germany, and 14.8% against France, followed by Italy (10.5%), Spain (10.1%), and Poland (8.9%).** The most impacted EU MSs shifted across the year, with France leading in Q1, Italy in Q2, Germany in Q3 and Denmark in Q4.

[591] hxxps://t.me/noname05716_eng_vers/354 (Accessed on 08-10-2025)
[592] hxxps://t.me/Darkstormteamback/112 (Accessed on 16-10-2025)
[593] hxxps://t.me/nnm05716english/352 (Accessed on 01-12-2025)
[594] hxxps://t.me/Keymous_main/324 (Accessed on 13-09-2025)
[595] hxxps://t.me/mrhamzaofficiel/1306 (Accessed on 08-10-2025)
[596] hxxps://t.me/nnm05716english/294 (Accessed on 24-11-2025)
[597] hxxps://t.me/DARKSTORM_UPDATE/211 (Accessed on 14-08-2025)
[598] hxxps://t.me/Darkstormteamnewteam/188 (Accessed on 15-10-2025)
[599] hxxps://t.me/nnm057_16/6238 (Accessed on 05-01-2025)
[600] hxxps://t.me/nnm057_16/6612 (Accessed on 01-02-2025)

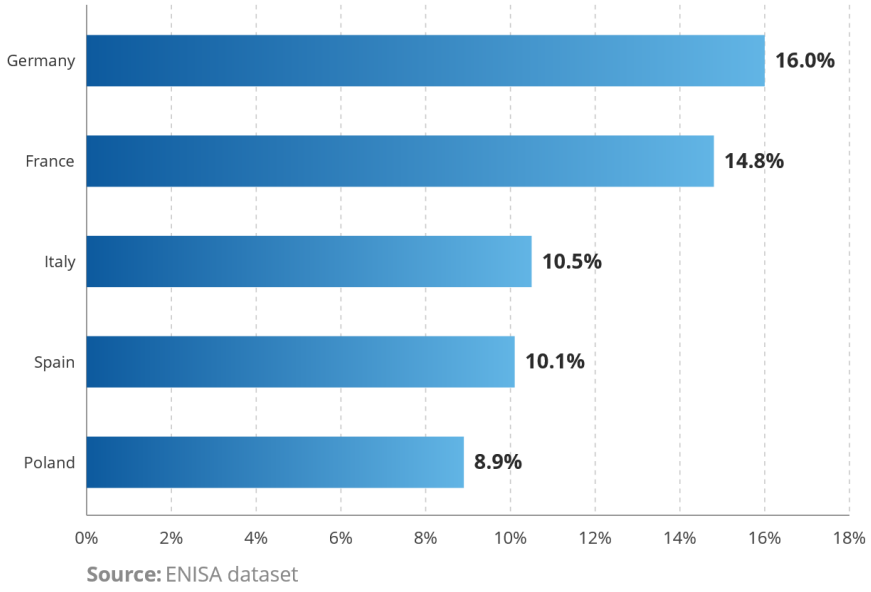


Figure 375 – Top 5 EU MS impacted by ideology driven claims

France, Italy, Lithuania, and Spain have been the most targeted Member States by hacktivists in Q1, often under named operation banners. The first surge of hacktivism attacks occurred in late February and early March, when Q1 activity rose above Q4 2024 levels. The surge was mainly on incidents claimed against Spain following their political support for Ukraine[601]. **Q1 also showed signs of ecosystem disruption and adaptation**, as hacktivist groups responded to Telegram takedowns with alias changes and migration away from the platform. ENISA saw that more than 60 hacktivist groups were removed from the Telegram platform by Telegram administrators between January and March following the arrest of Telegram's CEO in 2024[602].

Activity remained elevated in Q2. NoName057(16) was the most active hacktivist group while France, Germany, Poland and Lithuania were the most targeted EU MSs. Hacktivist activity was observed to be concurrent with political or geopolitical triggers such as the new security bill in Italy[603], the political situation in France[604], and legal actions from Lithuania against Belarus at the International Court of Justice over illegal immigration[605]. Q2 also showed retaliatory framing, including operations linked to support for Ukraine[606] [607] and the NATO Summit held in The Hague[608] [609] in June 2025.

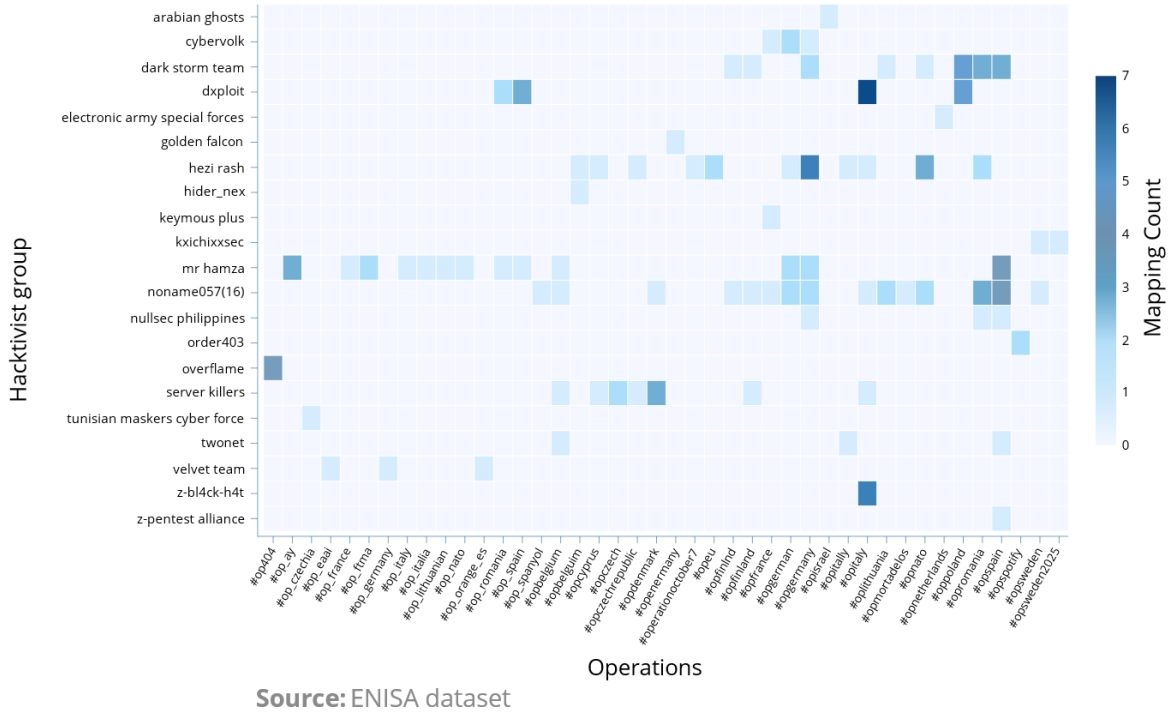
Hacktivist activity reached its highest level in Q3. This quarter was marked by a surge between mid-July and mid-August, shortly after the announcement of Operation Eastwood against NoName057(16)[610]. Germany became the main target, particularly under #OpGermany, while France,

[601] https://www.pravda.com.ua/eng/news/2025/02/28/7500740/
[602] https://www.lemonde.fr/pixels/article/2024/08/25/l-arrestation-en-france-de-pavel-durov-le-pdg-de-telegram-une-premiere-mondiale_6294313_4408996.html
[603] https://www.idea.int/democracytracker/report/italy/june-2025
[604] https://www.forbes.com/sites/mikeosullivan/2025/06/28/is-france-on-the-cusp-of-another-political-crisis/
[605] https://www.icj-cij.org/sites/default/files/case-related/200/200-20250717-ord-01-00-en.pdf
[606] https://www.lrt.lt/en/news-in-english/19/2562250/lithuanian-fm-calls-on-eu-to-act-boldly-after-it-agrees-on-new-russia-sanctions
[607] hxxps://t.me/NNM05716_Es_ver/73 (Accessed on 26-05-2025)
[608] https://www.nato.int/cps/en/natohq/235800.htm
[609] hxxps://t.me/Darkstormbackup2/275 (Accessed on 02-06-2025)
[610] https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network

Spain and Italy also remained targets. Public administration continued to be the primary target sector, but activity against transport increased compared with Q2.

Q4 activity declined from the Q3 peak but remained above early-year levels with NoName057(16) continuing to dominate the hacktivist landscape followed at a distance by Pro-Russia Server Killers and Pro-Palestine Dark Storm team. Denmark emerged as the most targeted Member State. The country demonstrated a strong willingness to support Ukraine[611] that caused repeated campaigns by Pro-Russia groups, notably in the context of the Danish elections[612]. Other EU MSs that were particularly targeted by hacktivists in Q4 were Belgium, France and Spain.

For the reporting period, the participation of hacktivist groups to coordinated campaigns, typically under the #op banner, is shown in Figure 56.



Source: ENISA dataset

Figure 56 - Hacktivist groups involved in coordinated campaigns against EU MSs

Pro-Russia NoName057(16) and pro-Palestine Hezi-rash, Mr Hamza and Dark Storm Team have been the most active groups regarding their participation to such campaigns against EU Member States.

[611] https://www.fmn.dk/en/news/2024/denmark-pushes-further-donations-to-ukraine-before-the-end-of-the-year/
[612] https://samsik.dk/artikler/2025/11/flere-partiers-hjemmesider-ramt-af-ddos-angreb/

6.4 Key trends

In 2025, Distributed Denial of Service (DDoS) remained the primary tactic, technique and procedure (TTP) for hacktivist activities affecting the EU. ENISA's analysis of DDoS activity linked to NoName057(16) and the DDoSia project[613] between July and November 2025 showed how hacktivist activity combined disruption, mobilisation and influence operations. DDoSia tasking relied on HTTP GET, SYN, ACK, POST, SYN-ACK, UDP flood, and ICMP ping methods, with concentration on TCP ports 443 and 80, consistent with targeting web services. However, in the case of NoName057(16) and the associated infrastructure of the DDoSia botnet, the combination of activities and narratives showed that hacktivist DDoS activity should not be assessed only through technical disruption. ENISA's analysis showed that NoName057(16)'s public claims generally aligned with intended targeting by DDoSia. Nevertheless, only 23.8% of the claims assessed were validated through independent third-party availability checks. This disparity suggests that some claims may have served an influence objective by inflating perceptions of operational impact, including instances where disruption could not be verified.

Another important finding, beyond NoName057(16) and the DDoSia infrastructure, is the growing use of **DDoS-as-a-Service (DDoSaaS)** models by hacktivist groups, likely driven by a lack of technical capability or infrastructure to independently conduct large-scale attacks and/or increase the intensity and scope of DDoS attacks by enrolling additional hacktivist groups. This reflects a broader shift toward the commoditisation of DDoS capabilities, where attack tools, botnets and operational support are increasingly outsourced or shared across loosely affiliated operators. Commercially available services—often referred to as 'booters' or 'stressers' such as Elite stress[614]—provide on-demand DDoS capabilities through user-friendly interfaces, enabling low-skilled groups to launch more advanced attacks by simply selecting a target and paying a fee. Originally marketed as legitimate network testing tools, these platforms are widely abused for malicious purposes, offering features such as scalable traffic generation, multiple attack vectors and subscription-based access models. As a result, the technical and financial barriers to entry for conducting disruptive cyber operations has been significantly reduced, enabling hacktivist groups to participate in high-impact campaigns without owning or managing dedicated infrastructure[615].

Other examples of the commoditisation of ideology-driven capabilities include the **Pro-Palestine Keymous+ and Mr Hamza** groups. In addition to their hacktivist operations, Keymous+ has been assessed to potentially operating as a DDoSaaS, offering attack capabilities to aligned groups or partners. Keymous+ leverages a combination of infrastructure sources to deliver coordinated campaigns, while also collaborating with other groups to amplify scale and impact. Mr Hamza operates under the Hacktivism-As-A-Service (HaaS) model, where individuals or groups package cyber operations—particularly DDoS attacks—into accessible services for politically motivated and ideology driven clients or affiliates[616] [617].

The 2025 landscape indicates that hacktivism has remained a predominantly reputational pressure point, mainly against public administration in the EU with some instances of operational impact also observed. In parallel, a subset of groups continued to claim access to industrial or Internet-exposed systems[618]. Although **OT disruption remained largely unverified**, the focus on these environments indicates that adversaries have a rising interest in exploiting configurations, interfaces, and credentials for operational effect or signalling.

[613] https://www.recordedfuture.com/research/anatomy-of-ddosia
[614] https://elitestress.st/
[615] https://www.imperva.com/learn/ddos/booters-stressers-ddosers/
[616] https://www.radware.com/blog/threat-intelligence/keymous-plus-a-new-hacktivist-collective-or-a-ddos-as-a-service-brand/
[617] https://www.linkedin.com/posts/techsigninc_cybersecurity-hacktivism-mrhamza-activity-7351194385423695872-PHuQ
[618] https://cyble.com/blog/hacktivists-critical-infrastructure-attacks-2025/

At a global level and not necessarily related to ideology driven attacks, DDoS activity in 2025 increased in scale and frequency and became a means of exerting pressure against Internet-facing services and infrastructure. In 2025, 47.1 million DDoS attacks were mitigated globally, more than double the volume in 2024, equivalent to an average of 5 376 attacks every hour. Growth occurred at the network layer, where 34.4 million attacks were mitigated in 2025, compared with 11.4 million in 2024[619].

Attack size increased during the year. In mid-May 2025, a 7.3 Tbps multi-vector attack delivered 37.4 TB in 45 seconds and targeted tens of thousands of destination ports on a single IP address[620]. By Q3, the Aisuru botnet, assessed at 1–4 million infected hosts, launched attacks above 1 Tbps and 1 Bpps, with peaks of 29.7 Tbps and 14.1 Bpps[621]. In Q4, activity was linked to Aisuru-Kimwolf, including a 31.4 Tbps attack lasting 35 seconds, while in late 2025 attack sizes were more than 700% above those observed in late 2024[622].

Attack patterns and targeting also changed over the reporting period. In Q3, 71% of HTTP DDoS attacks and 89% of network-layer attacks globally ended in under 10 minutes, reducing the effectiveness of mitigation and response models. In the second half of 2025, more than 8 million DDoS attacks were recorded across 203 countries and territories, with EMEA accounting for 3.3 million events. More than half of observed attacks were multi-vector, combining bandwidth-exhaustion[623] and state-exhaustion techniques[624], while attacks against DNS root servers and Network Time Protocol (NTP) services showed activity against core internet services[625]. In 2025, application layer (Layer 7) DDoS attacks reportedly exhibited an increase of 128% over the previous year. These attacks can generate disruption where traffic volumes appear modest. This is particularly relevant for services, Application Programming Interfaces (APIs), login flows, payment services and other user journeys where availability can be degraded without high traffic volumes[626].

[619] https://blog.cloudflare.com/ddos-threat-report-2025-q4/
[620] https://blog.cloudflare.com/defending-the-internet-how-cloudflare-blocked-a-monumental-7-3-tbps-ddos/
[621] https://blog.cloudflare.com/ddos-threat-report-2025-q3
[622] https://blog.cloudflare.com/ddos-threat-report-2025-q4/
[623] Bandwidth exhaustion attacks aim to overwhelm the victim's internet connection by flooding it with massive volumes of traffic (measured in Gbps/Tbps) to consume all available bandwidth so legitimate traffic cannot reach the service (https://www.netscout.com/what-is-ddos/state-exhaustion-attacks)
[624] State exhaustion attacks target the connection/state tables of firewalls, load balancers or servers by creating huge numbers of half-open or fake sessions. Instead of saturating bandwidth, they exhaust memory and processing resources needed to maintain network states. SYN floods are the classic example. (https://www.netscout.com/what-is-ddos/state-exhaustion-attacks).
[625] https://www.netscout.com/resources/threat-report
[626] https://app.stationx.net/articles/ddos-statistics

7. Vulnerabilities

The exploitation of vulnerabilities remains one of the most prevalent intrusion vectors. Specifically, the threat landscape in 2025 was characterised by confirmed attacks against enterprise infrastructure, edge devices and developer tooling as well as unpatched legacy IoT and edge devices (impacting among others D-Link, Zyxel, DASAN, Huawei, Realtek and Netgear devices) that have left many exposed[627]. Overall, attackers continued to successfully manage to achieve the weaponisation of newly disclosed vulnerabilities within a constantly decreasing time span[628].

ENISA as a CVE Program-Root

In line with Coordinated Vulnerability Disclosure practices in the EU[629] and complementary to its role as a Common Vulnerability and Exposure Numbering Authority (CNA)[630], ENISA maintains the European Vulnerability Database (EUVD)[631] to further support the cybersecurity community by providing reliable and timely information related to vulnerabilities. Since November 2025 ENISA has expanded its role in vulnerability management by becoming a Root CVE thus becoming a central point of contact within the CVE programme for national and EU authorities, EU CSIRTs network members and cooperative partners falling under ENISA's mandate.

Overall, more than **48 thousand new vulnerabilities** were published in 2025 with assigned Common Vulnerability and Exposure (CVE) Identifiers, a programme with the purpose of identifying, defining and cataloguing publicly disclosed cybersecurity vulnerabilities — a **22% increase** from the previous year.

627 https://www.vulnerability-lookup.org/2026/05/11/vulnerability-report-2025/
628 https://zerodayclock.com/
629 https://csirtsnetwork.eu/homepage?tab=cvd
630 https://www.enisa.europa.eu/topics/vulnerability-disclosure
631 https://euvd.enisa.europa.eu/homepage

A breakdown of the vulnerabilities in the Common Vulnerability Scoring System (CVSS[632]), a framework for rating the severity of software and hardware vulnerabilities, shows that **9% were Critical, 30% High, 49% Medium and 3% Low, while 9% remained unscored**.

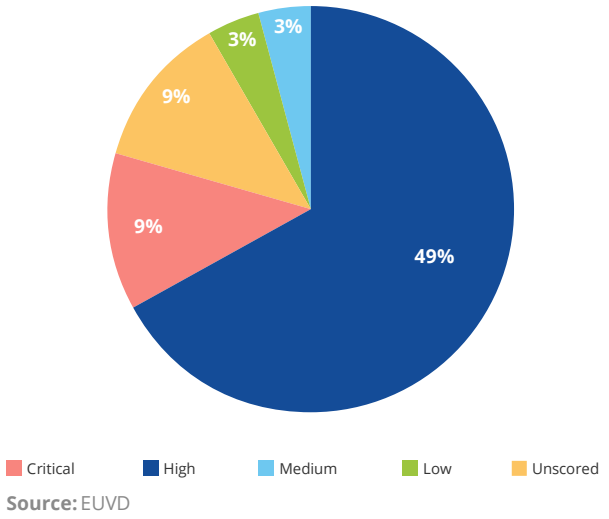


Figure 57 - CVSS Base Score Distribution per 2025's CVE data

When considering the attack surface, **71% of documented vulnerabilities mentioned *Network* as the attack vector**, in accordance with the definition of the CVSS Attack vector metric[633]. This underscores the potential risk of remote exploitation, especially for internet-facing systems.

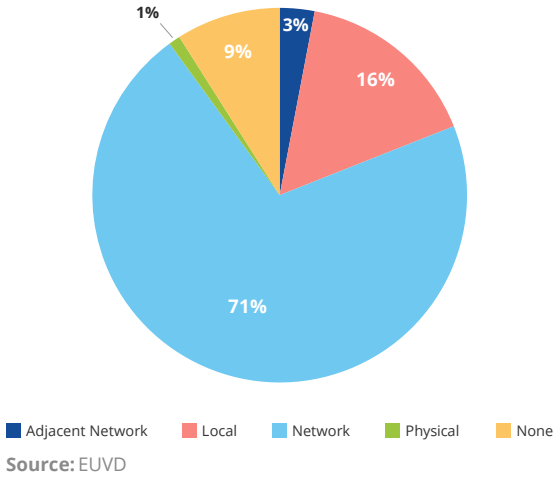


Figure 58 - Attack vectors of vulnerabilities identified in 2025

Based on the Common Weakness Enumeration (CWE) list, a community-developed category system for hardware and software weaknesses and vulnerabilities calculated by analysing public vulnerability

[632] Covering all versions used in reporting.
[633] https://www.first.org/cvss/specification-document

information in CVE Records for CWE root cause mappings[634], the top 10 most common weaknesses in hardware and software in 2025 were the following:

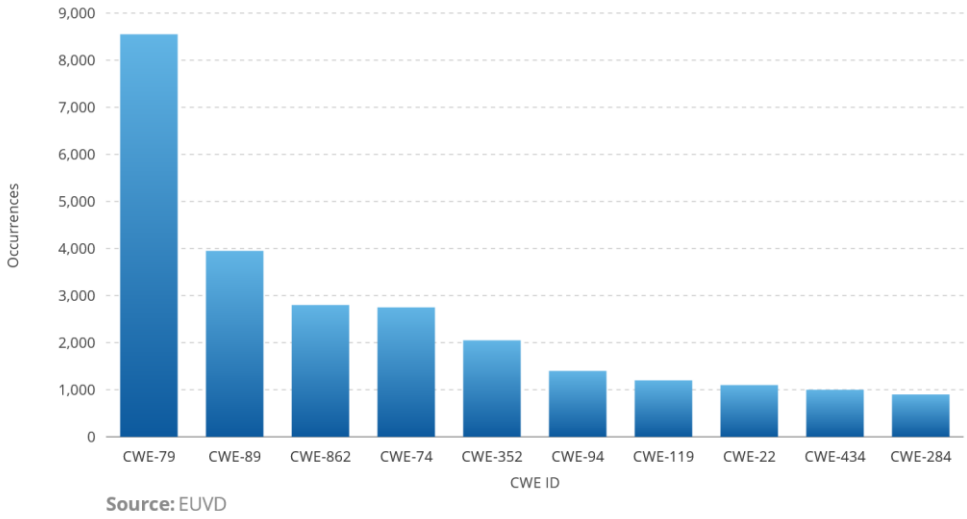


Figure 59 - Top 10 Most Common CWE (2025)

The CWE 2025 list[635] uses a scoring mechanism that indicates which weaknesses are common, have caused significant harm and could consequently have security ramifications. Building upon it, the top 25 most relevant weaknesses in hardware and software were the following:

Rank	ID	Name	Score	CVEs in KEV	Rank Change vs 2024
1	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	60.38	7	0
2	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28.72	4	+1
3	CWE-352	Cross-Site Request Forgery (CSRF)	13.64	0	+1
4	CWE-862	Missing Authorisation	13.28	0	+5
5	CWE-787	Out-of-bounds Write	12.68	12	-3
6	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	8.99	10	-1
7	CWE-416	Use After Free	8.47	14	+1
8	CWE-125	Out-of-bounds Read	7.88	3	-2
9	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7.85	20	-2
10	CWE-94	Improper Control of Generation of Code ('Code Injection')	7.57	7	+1
11	CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	6.96	0	N/A
12	CWE-434	Unrestricted Upload of File with Dangerous Type	6.87	4	-2
13	CWE-476	NULL Pointer Dereference	6.41	0	+8
14	CWE-121	Stack-based Buffer Overflow	5.75	4	N/A
15	CWE-502	Deserialisation of Untrusted Data	5.23	11	+1
16	CWE-122	Heap-based Buffer Overflow	5.21	6	N/A
17	CWE-863	Incorrect Authorisation	4.14	4	+1
18	CWE-20	Improper Input Validation	4.09	2	-6
19	CWE-284	Improper Access Control	4.07	1	N/A
20	CWE-200	Exposure of Sensitive Information to an Unauthorised Actor	4.01	1	-3
21	CWE-306	Missing Authentication for Critical Function	3.47	11	+4
22	CWE-918	Server-Side Request Forgery (SSRF)	3.36	0	-3
23	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	3.15	2	-10

[634] https://cwe.mitre.org/about/index.html
[635] https://cwe.mitre.org/top25/archive/2025/2025_cwe_top25.html#tableView.

24	CWE-639	Authorization Bypass Through User-Controlled Key	2.62	0	+6
25	CWE-770	Allocation of Resources Without Limits or Throttling	2.54	0	+1

Figure 60 - Top 25 CWEs identified in 2025

The top 20 vendors whose solutions were reported as vulnerable accounted for **34%** of all newly disclosed documented vulnerabilities over the reporting period.

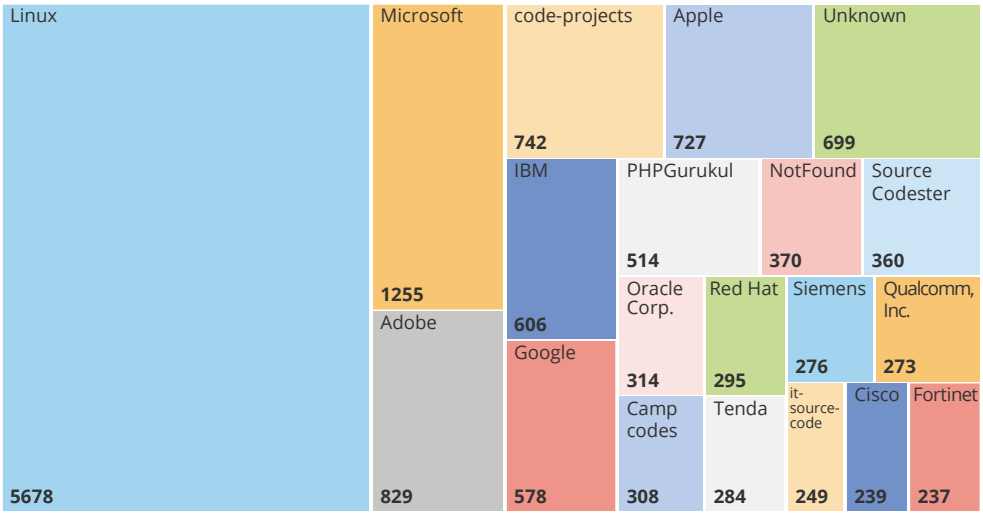


Figure 61 - Top 20 vendors by number of newly disclosed vulnerabilities in 2025

The **CISA's Known Exploited Vulnerabilities (KEV) Catalogue**[636] **added 245 vulnerabilities** over the reporting period, of which the top ten affected vendors are displayed in figure 62 below.

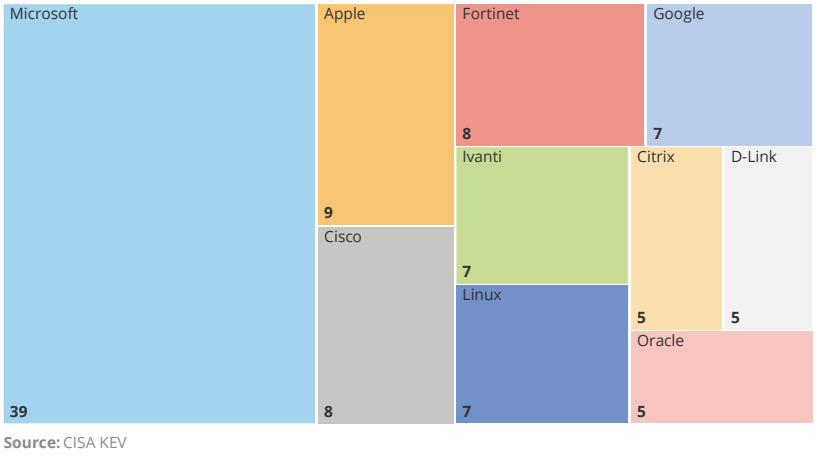


Figure 62 - Top 10 Vendors based on CISA KEV

[636] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

The top three most Common Weakness Enumeration (CWE) related to Known Exploited Vulnerabilities in the reporting period are:

- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'),
- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'),
- CWE-502: Deserialization of Untrusted Data.

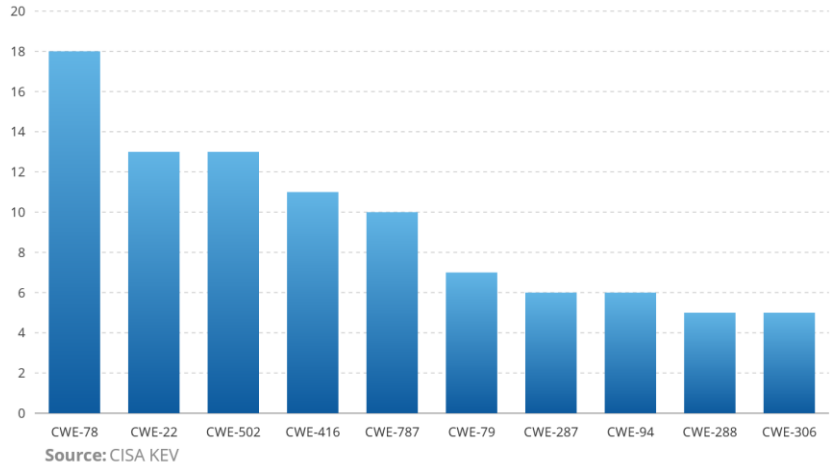


Figure 63 - Top CWEs based on CISA KEV

All these weaknesses can allow memory modification and code execution (which could lead to taking full control of the impacted system) as well as crashes and denials of service impacting the availability of the services run on or through the impacted systems.

A dynamic list of *knowingly exploited vulnerabilities* is accessible via the ENISA EUVD[637]. It notably merges EU and CISA KEV Catalogues.

[637] https://euvd.enisa.europa.eu/search?exploited=true

8. Outlook and conclusion

Current observations indicate that **several of the dynamics documented during the reporting period are likely to persis**t. In the near-term, it is highly likely public and private organisations in EU MSs will continue to face hacktivist-associated threats with periodic peaks, stable cyberespionage activities with a continued prevalence of Russia-nexus and China-nexus intrusion sets, and an even more mature yet further fragmented and resilient cybercriminal ecosystem.

The activity observed during 2025 suggests that the cyber threat landscape affecting the EU is becoming increasingly shaped by the interaction between established threats, as well as the emergence of new groups. Cybercriminal, hacktivist and State-nexus groups continued pursuing different objectives, yet frequently relied on similar access vectors, tools and operational approaches. Still, new groups will likely continue emerging. Of note, the frequent updates and convergence of TTPs by well-known State-nexus and cybercriminal groups increasingly hinder tracking and consistent imputation, ultimately leading to a virtually inflated and scattered threat landscape.

Cybercrime will highly likely remain one of the most impactful threats to business continuity for organisations operating in the EU as well as EU organisations operating abroad, ultimately having an economic impact on the EU market. Displaced or disrupted RaaS brands will continue being rapidly replaced by emerging programmes. Extortion schemes and breaches will likely continue evolving in line with changing technologies (including but not limited to AI) and monetisation opportunities. The continued availability of cybercriminal services, including tooling and operational support will further contribute to lowering barriers of entry to the cybercriminal ecosystem.

Another development is the **continued convergence of operational practices across different threat group types**. While assessed objectives appear distinct, the practical differences between cybercrime, hacktivist and State-nexus activity are likely to further converge. The same vulnerabilities, platforms and toolsets are likely to be leveraged regardless of the groups' motivation. As a result, organisations may increasingly face different threats gaining unauthorised access through similar pathways, reinforcing the importance of addressing common weaknesses in addition to efforts to increase collective situational awareness.

Several incidents documented during the reporting period also confirmed the well-established critical importance of digital dependencies. Software suppliers, developers, managed service providers, cloud platforms and customer-service environments continued to appear as high-value targets to enable upstream and downstream impact. As organisations continue integrating third-party services into their operations, **opportunities for threat groups to achieve broader impact through a single compromise are likely to increase**.

2025 also showed that social engineering continues to evolve. While large-scale phishing and spearphishing remain common threats, campaigns increasingly relied on trusted communication platforms and bypassing or abusing legitimate authentication mechanisms. Device-code phishing and ClickFix illustrate a **broader shift towards techniques designed to further capitalise on abusing trust** rather than technical weaknesses alone.

Geopolitical developments are also likely to remain a major driver of cyber activity affecting the EU. Throughout the reporting period, disruptive and cyberespionage campaigns frequently coincided with political developments, public statements or high-visibility events. Similar patterns are likely to persist. Cyber operations continue to offer a relatively low-cost means of signalling intent, attracting

attention and exerting pressure without crossing the threshold of conventional conflict. While State-nexus groups are likely to maintain a sustained interest in public administration and other high value targets across the EU, hacktivist-led DDoS will persist as a nuisance, both in terms of the potential disruption of business continuity and in the information operation sphere, highly likely with spikes around high visibility events and announcements by EU MSs and Union entities and authorities. While claims pertaining to the targeting of Operational Technology by hacktivist groups will likely increase, confirmed incidents resulting in operational impact are likely to remain stable.

Looking ahead, ENISA's assessment is that Artificial Intelligence is likely to further accelerate several of these developments. During 2025, ENISA observed AI being incorporated into the playbooks of cybercriminal, State-nexus and information manipulation sets, although often in a supporting role rather than as a primary capability. This is highly likely to change as so-called 'frontier models' would become more widely available. While **AI will highly likely continue to primarily act as a force multiplier, it is also likely 2026 will 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, which would be likely to hinder detection and imputation for networks defenders.

Appendix A Law Enforcement Authorities operations in the EU

Date	LEA Action taken	Results / Impact of Operation	Involved countries/entities
28/01/2025	OP Talent - Takedown of Cracked and Nulled platforms users in total[638]	2 suspects arrested 7 properties searched 17 servers, 12 domains and 50 devices seized EUR 300 000 in cash and cryptocurrencies seized Take down of a financial processor	France, Germany, Greece Italy, Romania and Spain, along with Australian Federal Police and US Department of Justice (DoJ) and Federal Bureau of Investigation (FBI)
01/02/2025	Arrest of an actor who allegedly caused millions of euros in damage to dozens of victims around the globe[639]	Arrest of the main suspect	France, US
05/02/2025	Arrest of suspect for cyberattacks who allegedly participated in over 40 attacks against Spanish Defence Ministry, NATO systems and US Army to access sensitive data[640]	Arrest of the main suspect	Spain, US FBI
10/02/2025	Arrest of key figures behind Phobos and 8Base ransomware[641]	27 servers taken down 400+ companies worldwide warned of ongoing attacks No further 8Base claims observed after the operation	Belgium, Czechia, France, Germany, Poland, Romania, Spain, Sweden, Japan, Singapore, Switzerland, Thailand, United Kingdom, US
26/02/2025	Operation Cumberland - targeting AI-generated Child Sexual Abuse Material (CSAM)[642]	273 suspects identified 25 suspects arrested 33 house searches 173 electronic devices seized	Austria, Belgium, Czechia, Denmark, Finland, France, Germany, Hungary, The Netherlands, Poland, Spain, Sweden, Australia, Bosnia & Herzegovina, Iceland, New Zealand, Norway, Switzerland, United Kingdom
07/05/2025	Operation PowerOFF - Takedown of 6 stresser/booter services[643]	Takedown of 6 major DDoS-for-hire platforms[644] Arrest of 4 individuals Seizure of 9 domains	Poland, Germany, the Netherlands, US
09/05/2025	Op Moon - Dismantling of a botnet (Anyproxy and 5socks)[645]	Seizure of domains disabled botnet's activity Arrest of 4 individuals Successful remediation of vulnerabilities in compromised devices	The Netherlands, US, Thailand

[638] https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-takes-down-two-largest-cybercrime-forums-in-world
[639] https://www.justice.gov/usao-sdny/pr/serial-hacker-intelbroker-charged-causing-25-million-damages-victims
[640] https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=16448#
[641] https://www.europol.europa.eu/media-press/newsroom/news/key-figures-behind-phobos-and-8base-ransomware-arrested-in-international-cybercrime-crackdown
[642] 25 arrested in global hit against AI-generated child sexual abuse material | Europol.
[643] https://www.europol.europa.eu/media-press/newsroom/news/ddos-for-hire-empire-brought-down-poland-arrests-4-administrators-us-seizes-9-domains
[644] cfxapi, cfxsecurity, neostress, jetstress, quickdown, and zapcut
[645] https://www.justice.gov/usao-ndok/pr/botnet-dismantled-international-operation-russian-and-kazakhstani-administrators

12/05/2025	Arrest of a suspect carrying out DoppelPaymer ransomware attacks[646]	Seizure of suspect's devices Initiation of extradition process to the Netherlands Part of a larger operation against DoppelPaymer operation Suspect was allegedly responsible for an attack on a Dutch Research Council (NOW) that caused approximately 4.5 million EURO in damages	The Netherlands, Moldova
19/05/2025	Operation Endgame - Dismantling of key infrastructure behind malware to launch ransomware attacks[647]	300 servers were taken down globally neutralizing 650 domains Issuing of arrest warrants against 20 targets Seizure of EUR 3.5 million in cryptocurrency Neutralisation of seven malware strains (Bumblebee, Lactrodectus, Qakbot, Hijackloader, Danabot, Trickbot, Warmcookie)	Denmark, France, Germany, Netherlands, UK, Canada, US
21/05/2025	Operation Macefall - Global takedown of Lumma Stealer malware infrastructure[648]	2 300 domains blocked Seizure of Lumma control panel Identification of 394 000 infected Windows systems globally	Europol EC3, Japan (JC3), US DoJ
27/05/2025	Operation Endgame [649]	Dismantling of crypting and Counter Anti-Virus (CAV) services	Finland, the Netherlands, US
23/06/2025	Arrest of hacking forum (BreachForums) operators[650]	4 individuals using the online aliases 'ShinyHunters', 'Hollow', 'Noct' and 'Depressed' for their involvement in operating BreachForums	France
25/06/2025	Crypto investment fraud group dismantled in Spain after defrauding 5 000 victims worldwide[651]	5 arrests	Spain, Estonia, France, US
14/07/2025	Operation Elicius	Identification of suspects linked to Disktation ransomware	Italy, France, Romania
23/07/2025	Operation Ratatouille[652]	Arrest of the xx.is admin	France, Ukraine, Europol EC3
07/08/2025	Operation Checkmate[653]	Dismantling of BlackSuit ransomware infrastructure	Germany, Lithuania, the Netherlands, US

[646] https://www.bleepingcomputer.com/news/security/moldova-arrests-suspect-linked-to-doppelpaymer-ransomware-attacks/
[647] https://www.europol.europa.eu/media-press/newsroom/news/operation-endgame-strikes-again-ransomware-kill-chain-broken-its-source
[648] https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world%E2%80%99s-largest-infostealer-lumma
[649] https://www.justice.gov/usao-sdtx/pr/websites-selling-hacking-tools-cybercriminals-seized
[650] https://www.bleepingcomputer.com/news/security/breachforums-hacking-forum-operators-reportedly-arrested-in-france/
[651] https://www.europol.europa.eu/media-press/newsroom/news/crypto-investment-fraud-ring-dismantled-in-spain-after-defrauding-5-000-victims-worldwide
[652] https://www.europol.europa.eu/media-press/newsroom/news/key-figure-behind-major-russian-speaking-cybercrime-forum-targeted-in-ukraine
[653] https://www.ice.gov/news/releases/ice-washington-dc-leads-international-takedown-blacksuit-ransomware-infrastructure

16/09/2025	Arrest of a UK citizen allegedly linked to Scattered Spider[654]	Arrest of the main suspect	United Kingdom, the Netherlands, Romania, Canada, Australia, US
10/10/2025	Cybercrime-as-a-service takedown: 7 arrested[655]	Seizure of around 1 200 sim boxes devices that operated some 40 000 SIM cards	Austria, Estonia, Latvia, Europol
24/11/2025	Shut down of Cryptomixer[656]	Seizure of over 12 TB of data and more than EUR 25 million in Bitcoin	Germany, Switzerland, Europol

654 https://www.justice.gov/opa/pr/united-kingdom-national-charged-connection-multiple-cyber-attacks-including-critical
655 https://www.europol.europa.eu/media-press/newsroom/news/cybercrime-service-takedown-7-arrested/
656 https://www.europol.europa.eu/media-press/newsroom/news/europol-and-partners-shut-down-cryptomixer

Appendix B Assessment methodology

CONFIDENCE LEVEL	SYNONYMS
●●●●● HIGHLY LIKELY	High confidence. >90%
●●●●○ LIKELY	Moderate to high confidence. 60 - 90%
●●●○○ POSSIBLE	Moderate confidence. 40 - 60%
●●○○○ PLAUSIBLE	Low to moderate confidence. 10 - 40%
●○○○○ UNLIKELY	Low confidence. <10%

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.

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