EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA THREAT LANDSCAPE 2025

OCTOBER 2025

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

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

AUTHORS

Jamila BOUTEMEUR, Ifigeneia LELLA, Ilias BAKATSIS, Georgios CHATZICHRISTOS, Kevin FOLEY, Jussi LESKINEN, Jakub OTCENASEK, Dominik ZIOLEK, ENISA.

EEAS STRATCOM.

CONTRIBUTORS

The ENISA Threat Landscape authors would like to express their appreciation to the EEAS STRATCOM and Europol EC3 colleagues, as well as the ENISA Incident and Vulnerability reporting services (IVS) and CIRCL colleagues for their active support to the report.

ACKNOWLDGEMENTS

The ENISA Threat Landscape authors would like to acknowledge the valuable feedback and validation of the members of the National Liaison Officers (NLO) network, of the CSIRTs Network (CNW), and of the ENISA Cyber Partnership Programme, as well as the comments received from our European Union Aviation Safety Agency (EASA) colleagues, I4C+ (Information and Analysis Center for Cities), the Financial Services Information and Analysis Center (FI-ISAC), and the European Rail Operators Information and Analysis Center (Rail-ISAC).

We also want to thank our ENISA colleagues, Apostolos MALATRAS, Stefano DE CRESCENZO , Razvan GAVRILA, Erika MAGONARA, Eleni PHILIPPOU, Edgars TAURINS, and Johannes CLOS for their input and overall support.

LEGAL NOTICE

Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication.

Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

ISBN:978-92-9204-723-8 ISSN: 2363-3050 DOI: 10.2824/1946374

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

This year's ENISA Threat Landscape (ETL) introduces a **revised and concise format** designed to deliver insights through a **threat-centric approach** and enhanced contextualisation. This edition integrates additional analysis of adversary behaviours, vulnerabilities and geopolitical drivers, aimed at both strategic and operational audiences, offering an actionable perspective on trends shaping the EU's cyber threat environment.

The ETL 2025 provides **an overview of the European cyber threat ecosystem from July 2024 to June 2025**, drawing on nearly 4 900 selected and curated incidents. The reporting period highlights a maturing threat environment characterised by rapid exploitation of vulnerabilities and growing complexity in tracking adversaries.

Intrusion activity remains significant, with ransomware at its core. Cybercriminal operators notably responded to the actions of law enforcement by decentralising operations, adopting aggressive extortion tactics and capitalising on regulatory compliance fears. The continuous proliferation of ransomware-as-a-service models, builder leaks and the services of access brokers has further lowered barriers to entry and diversified ransomware families, fuelling a professionalised and resilient criminal ecosystem.

In parallel, **state-aligned threat groups intensified their long-term cyberespionage campaigns** against the telecommunications, logistics networks and manufacturing sectors in the EU, demonstrating advanced tradecraft such as supply chain compromise, stealthy malware frameworks and abuse of signed drivers.

Hacktivist activity continues to dominate reporting, representing almost 80% of recorded incidents and driven primarily by low-level distributed denial-of-service operations. While overall resulting in very low impact, these campaigns demonstrate how low-cost tools are scaled for ideology-driven operations.

Sectoral targeting patterns reinforce the EU' systemic exposure. **Public administration networks remain the primary focus** (38%), notably for hacktivists and state-nexus intrusion sets, while transport emerged as a high-value sector, particularly maritime and logistics. Aviation and freight operations have faced ransomware disruptions, while digital infrastructure and services remain strategic targets for both cyberespionage and ransomware operators.

Phishing remains the dominant intrusion vector (60%) and is evolving through techniques used in large-scale campaigns. The availability of phishing-as-a-service platforms demonstrates the industrialisation of phishing operations, enabling adversaries of all skill levels to launch complex campaigns. Abuse of cyber dependencies have also intensified, as shown by compromises in open-source repositories, malicious browser extensions and breaches of service providers, amplifying risk throughout interconnected digital ecosystems.

Across all campaigns, adversaries continue to rely on a consistent set of tactics, techniques and procedures. **Vulnerability exploitation remains a cornerstone of initial access** (21.3%), with widespread campaigns rapidly weaponising them within days of their disclosure—underscoring the need to ensure patch availability and to implement and enforce basic measures for cyber hygiene.

Artificial intelligence has become a defining element of the threat landscape. By early 2025, AI-supported phishing campaigns reportedly represented more than 80 percent of observed social engineering activity worldwide, with adversaries leveraging jailbroken models, synthetic media and model poisoning techniques to enhance their operational effectiveness.

The threat landscape depicted in this edition reflects how **the cyber threat landscape is shifting toward mixed, possibly convergent pressure**, with fewer single high impact incidents, and more continuous, diversified and convergent campaigns that collectively erode resilience.

2. METHODOLOGY

The ENISA Cybersecurity Threat Landscape (ENISA CTL) updated methodology published in August 2025[1] was used to write the ETL.

For the purpose of the ETL 2025 report, ENISA analysts collected and analysed 4 875 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 referred to spans from 1 July 2024 to 30 June 2025, with the cut-off date being 30 June 2025.

As much as possible, primary sources are referenced in footnotes to substantiate ENISA's analysis and assessments. ENISA appreciate 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 depth and temporality. For instance, vague sectorial or geographic reporting (i.e., 'private companies', 'Europe') is likely to impact ENISA's dataset. Another caveat is the proper sectorial categorisation, especially when one incident impacts an organisation operating in multiple sectors. To avoid inflating the threat, ENISA analysts proceeded to 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.

It should be noted that incidents are not necessarily reported immediately or confirmed in open sources. For instance, where ransomware and DDoS are more immediate 'visible' threats, often claimed directly by their operators, cyberespionage campaigns are typically documented with a delay spanning from 6 months to more than 4 years. It should also be noted that, to some extent, increased reporting of a specific threat does not necessarily reflect an increased tempo but rather speaks to the audience's interest.

The incidents analysed in the Foreign Information Manipulation and Interference (FIMI) section have been shared by the European External Action Service (EEAS) and based on the strategic FIMI monitoring efforts of the EEAS. They reflects patterns seen in known sources related to overt FIMI, or independently imputed operations by selected actors and on priority issues of the EEAS. The totality of the incidents used in the EEAS sample refers to activities suspected to be linked to Russian Information Manipulation Sets to different degrees. Data on cyber-related FIMI activities by other threat groups are not systemically collected. The evidence presented serves illustrative purposes and should not be used to draw conclusions about general trends in FIMI, as it reflects only a limited subset of threat actors' activity.

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 assessments, words of estimative probability are used, with a matrix available in the Appendix.

Finally, the association of a threat with a particular nexus is solely based on attribution done by national authorities globally, and imputation (aka technical attribution) achieved by trusted private vendors, all referenced accordingly.

[1] https://www.enisa.europa.eu/sites/default/files/2025-08/ENISA%20CTL%20Methodology_Updated%20August%202025.pdf
[2] https://www.enisa.europa.eu/topics/cyber-threats/situational-awareness/enisa-cyber-partnership-programme-cpp

3. THREAT LANDSCAPE OVERVIEW

Based on the analysis of the dataset, social engineering tactics remain the primary entry point for threat actors, with phishing (including vishing, malspam, and malvertising) accounting for about 60% of observed cases. Exploitation of vulnerabilities (21.3%) remains a prevalent intrusion vector, followed by botnets (9.9%). Malicious applications represent 8%, showing that compromised or trojanised software and applications continue to play a role in system intrusions, while unauthorised access by insider threats (0.8%) contribute smaller but still relevant shares. Overall, the distribution underscores that while phishing dominates the threat landscape, technical exploits, malware delivery mechanisms and insider risks remain meaningful concerns.

The data shows clear contrasts between phishing and vulnerability exploitation as intrusion vectors. While phishing is the most common pathway, its impact is diverse. Approximately 73% of phishing cases are classified as unknown, reflecting unclear or varied follow-up of malicious activities, and 27% led to intrusions. In terms of payloads, phishing leads to the deployment of malicious code in 23% of cases, suggesting it might be primarily used for malware-less objectives. Vulnerabilities, on the other hand, show a more focused risk profile. Nearly 70% of vulnerability cases culminate in intrusions, with 30% categorised as unknown, and 68% of these vulnerability-based incidents result in the deployment of malicious code, indicating that the exploitation of vulnerabilities is often a direct precursor to the installation of malware.

Fig. 1 - Most identified initial infection vector.
Source: ENISA dataset

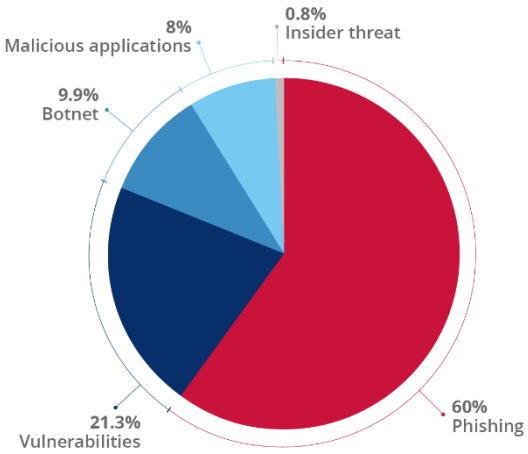
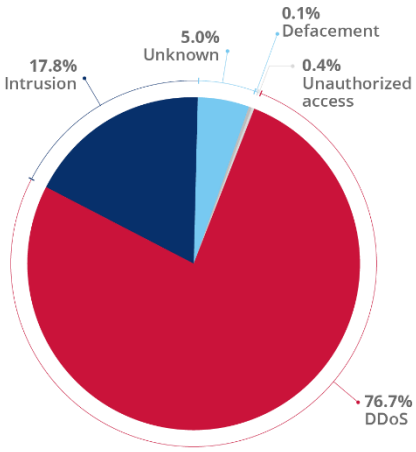


Fig. 2 - Distribution of incident types.
Source: ENISA dataset



The distribution of incident types is dominated by DDoS attacks, which make up about 76.7% of recorded cases. This category is overwhelmingly driven by hacktivist groups, which account for the majority of collected DDoS incidents, with cybercrime groups contributing a marginal fraction, often tied to extortion (e.g., ransom DDoS). Intrusions follow with 17.8%, dominated by cybercriminal activities, followed by state-aligned intrusion sets, which typically pursue persistence. Hacktivists appear only marginally in intrusion cases. Defacements were almost exclusively associated with hacktivists, underlining their role as a symbolic tactic for visibility and protest rather than a sustained intrusion method.

The prevalence of cybercriminal-led intrusions is illustrated through the type of malicious code deployed following intrusions, as well as the outcome of recorded intrusions. The combined share of ransomware, banking trojan, and infostealers accounts for 87.3% of these intrusions.

Fig. 3 - Distribution of identified malicious codes.
Source: ENISA dataset

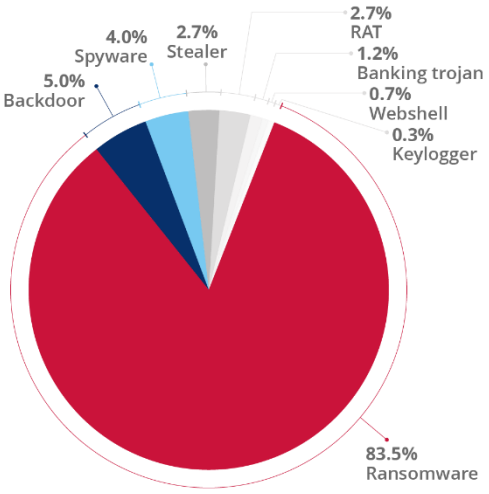
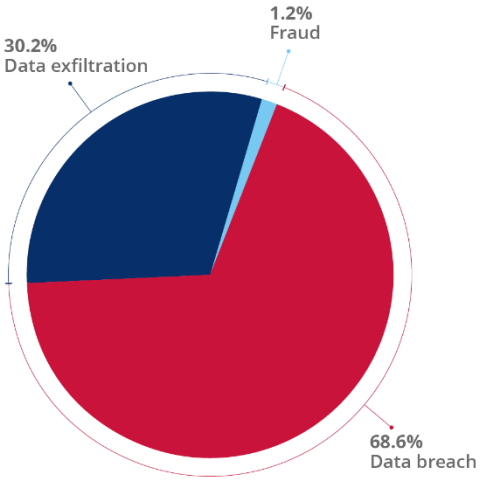


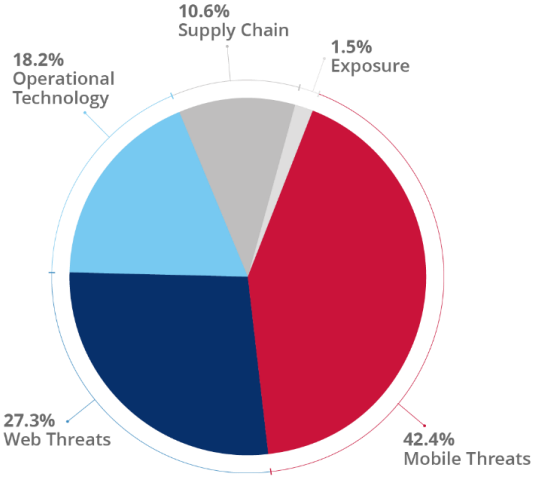
Fig. 4 - Outcome of identified intrusions.
Source: ENISA dataset



Out of recorded intrusions, 68.6% led to data breaches leaked on cybercriminal forums for sale, including 2.8% of these advertised breaches being presented as a direct outcome of a ransomware attack. Data exfiltration, including credential theft (8.9%) and strategic data collection (21.3%) accounted for 30.2%.

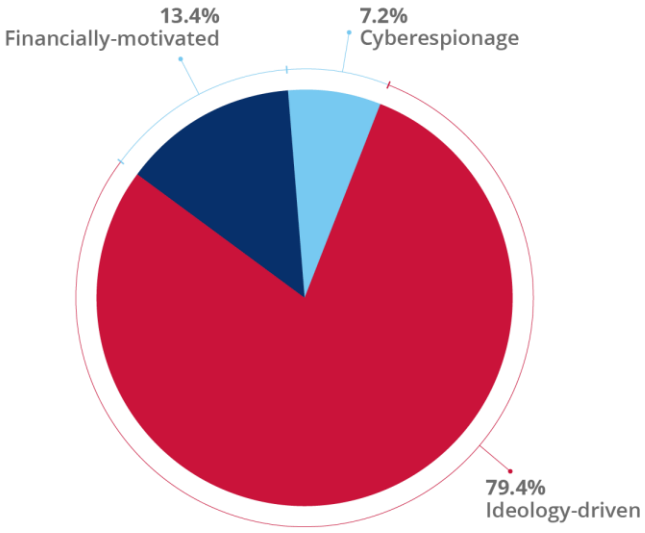
The distribution of threat categories shows a clear concentration in a few areas. Mobile threats account for the largest share at 42.4%, highlighting how mobile devices continue to be a primary attack surface. Web threats follow with 27.3%, underlining the persistent exploitation of online services and applications. Operational technology threats represent 18.2%, reflecting the growing exposure of industrial and critical systems as they continue being increasingly connected and targeted. Supply chain risks make up 10.6%, showing that attackers are actively leveraging indirect pathways through third-party providers and dependencies.

Fig. 5 - Distribution of threats.
Source: ENISA dataset



Based on assessed objectives, cyber activities targeting or impacting the EU mostly pertained to ideology-driven incidents exclusively carried out by hacktivists through DDoS. Financially motivated operations were primarily carried out by cybercriminal operators, while a few cases were associated to hacktivist groups, and state-aligned threats. Finally, cyberespionage campaigns accounted for 7.2%.

Fig. 6 - Distribution of assessed objectives.
Source: ENISA dataset



4. GENERAL KEY TRENDS

4.1 PHISHING REMAINS A PRIMARY INITIAL INTRUSION VECTOR

Phishing continued to be the primary method for initial intrusion, remaining an effective technique to carry out credential theft, session hijacking, payload deployment or command execution.

ClickFix-style scams appeared during the reporting period with the technique gaining momentum in Q1 2025 for both cybercriminal and state-aligned intrusion sets[3], often disguised as fake CAPTCHA prompts on compromised or fraudulent websites. These overlays tricked users into executing PowerShell commands under the pretext of human verification, leading to the installation of information stealers and loaders[4] [5].

Another innovative technique was the weaponisation of compromised WordPress sites to distribute info-stealers through drive-by downloads. From Q2 2025, threat actors embedded fake CAPTCHA and verification prompts into compromised websites to lure users into executing malicious payloads. The ClearFake campaign saw the distribution of credential-stealing malware including Lumma and Vidar, resulting in 9 300 confirmed infections[6]. These campaigns leveraged legitimate browser interfaces and social engineering to create convincing lures.

Phishing-as-a-Service (PhaaS) platforms, designed to automate the generation of branded phishing kits by cloning login pages and distributing links through templated infrastructure, enable low-skill operators to emulate trusted brands. This is illustrated by the Darcula platform, seen impersonating more than 200 organisations, whose services were seen leveraged to target victims in more than a hundred countries[7] [8]. Another PhaaS called Lucid expanded their portfolio by supporting phishing campaigns via mobile messaging services—iMessage and RCS— enabling over 169 targets in 88 countries[9] to be reached. Additional PhaaS developments include FlowerStorm, an adversary-in-the-middle kit mimicking Microsoft 365 portals and bypassing MFA[10].

Enabling endpoint protections evasion and email filtering, **QR code phishing** (aka quishing) was also reportedly seen, as observed in the Scanception campaign, where malicious QR codes embedded in PDF attachments were aimed at redirecting victims to credential harvesting pages hosted on trusted cloud platforms; these targeted users globally, including in the EU[11] [12].

4.2 INCREASINGLY TARGETED CYBER DEPENDENCIES

During 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[13] [14]. In mid-2024, the cyberespionage campaign Operation Digital Eye targeted professional IT providers in Southern Europe, aiming to infiltrate supply chains. Compromise attempts were reportedly unsuccessful[15]. In March 2025, Plus Service, an external provider managing the Telemaco platform for multiple Italian transport companies suffered a data breach involving unauthorised exfiltration to a remote cloud, prompting temporary access restrictions while remediation was carried out. This notably resulted in the Mobilita di Marca (MoM) ticketing systems being paralysed for two days, impacting several thousand commuters[16]. The same campaign

[3] https://www.proofpoint.com/us/blog/threat-insight/around-world-90-days-state-sponsored-actors-try-clickfix
[4] https://www.proofpoint.com/us/blog/threat-insight/clipboard-compromise-powershell-self-pwn
[5] https://blog.sekoia.io/clickfix-tactic-the-phantom-meet/
[6] https://thehackernews.com/2025/03/clearfake-infects-9300-sites-uses-fake.html
[7] https://lbttechgroup.com/index.php/blog/new-darcula-phishing-service-targets-iphone-users-via-imessage?tmpl=component&print=1&format=print
[8] https://www.beyondidentity.com/resource/darcula-phishing-as-a-service-platform-that-autogenerates-branded-kits
[9] https://thehackernews.com/2025/04/lucid-phaas-hits-169-targets-in-88.html
[10] https://www.darktrace.com/blog/from-rockstar2fa-to-flowerstorm-investigating-a-blooming-phishing-as-a-service-platform
[11] https://cyble.com/blog/scanception-a-qriosity-driven-phishing-campaign/
[12] https://www.darkreading.com/endpoint-security/criminals-send-qr-codes-phishing
[13] https://www.scworld.com/brief/cbs-affiliate-purportedly-compromised-by-lynx-ransomware-gang
[14] https://news.sophos.com/en-us/2025/05/27/dragonforce-actors-target-simplehelp-vulnerabilities-to-attack-msp-customers/
[15] https://www.sentinelone.com/labs/operation-digital-eye-chinese-apt-compromises-critical-digital-infrastructure-via-visual-studio-code-tunnels/
[16] https://www.tribunatreviso.it/cronaca/mon-hacker-attacco-biglietti-xueo4que

impacted the Busitalia Veneto app and subscription portal, and ATM Milano[17] [18]. Other relevant examples include the targeting of Berliner Verkehrsbetriebe (BVG)'s external service provider in May 2025, affecting the data of 180 000 BVG customers[19], and unauthorised access to Spanish energy company Repsol's customers, resulting from the compromise of one of the company's providers[20].

Adversaries were also seen **exploiting the digital supply chain**, notably by compromising software, repositories or browser extensions[21]. Since 2022, and increasingly observed over the reporting period, DPRK-nexus Lazarus leveraged supply chain compromise, with its most recent activities pertaining to the deployment of malicious Node Package Manager (npm) packages in GitHub repositories, mimicking legitimate libraries to compromise developers' environments[22] [23] [24]. Of note, repositories remain particularly exposed to secret sprawls stemming from insufficient protection with detected secrets reportedly increasing by 25% between 2023 and 2024[25]. A surge in attacks leveraging malicious browser extensions was observed in late 2024, with a campaign that compromised multiple companies' Chrome browser extensions; these notably targeted extensions related to Artificial Intelligence and Virtual Private Networks (VPN)[26] [27] [28] [29].

4.3 CONTINUOUS TARGETING OF MOBILE DEVICES

Q1 2025 observed an increased level of reporting pertaining to the targeting of mobile devices, with Android devices facing a higher level of threat.

Q3 2024 reportedly saw an uptick in the **exploitation of outdated devices** by the deployment of the Rafel RAT, primarily targeting Android devices for financially-motivated and cyberespionage purposes, notably in Czechia, France, Germany, Italy and Romania[30], as well as the re-emergence of the Medusa banking trojan updated with new features, and expanding their victimology to France and Italy[31]. Medusa was notably observed focusing on On-Device Fraud (ODF) through Account Takeover (ATO). Leveraging the same technique, BingoMod RAT was observed draining bank accounts and wiping devices, a concerning evolution[32].

Android **spyware for surveillance purposes used by State-aligned intrusion sets were also increasingly documented**, with Reaper's Android spyware KoSpy[33], or Android spyware BoneSpy and PlainGnome leveraged by Uzbekistan-nexus Sandcat. Of particular interest is a report documenting EagleMsgSpy, a legal intercept surveillance program targeting Android devices, reportedly developed by Wuhan Chinasoft Token Information Technology Co., Ltd. and used by Chinese Public Security Bureaus since at least 2017[34]. In February, multiple cybersecurity vendors published reports pertaining to the targeting of mobile devices by Russia-nexus intrusion sets. Google Threat Intelligence Group (GTIG) reportedly observed Sandworm, UNC5792, UNC4221 (aka UAC-0185) targeting the WhatsApp, Signal and Telegram accounts of individuals in Ukraine[35]. Notably Sandworm was observed enabling Russian military forces to connect Signal accounts on devices collected on the battlefield to actor-controlled infrastructure for follow-on exploitation. Sandworm was also observed abusing the 'linked devices' feature, by crafting malicious QR codes to link a victim's account to an actor-controlled Signal instance, and operating WAVESIGN. Volexity and Microsoft also reported on the

[17] https://www.fsbusitalia.it/it/veneto/news-veneto/2025/4/9/comunicazione-di-una-violazione-dei-dati-personali-agli-interess.html
[18] https://www.atm.it/it/AtmNews/AtmInforma/Pagine/comunicazioneutentiappATM.aspx
[19] https://www.bvg.de/de/unternehmen/medienportal/pressemitteilungen/2025-05-15-statment-it-angriff-dienstleister
[20] https://www.publico.es/economia/repsol-sufre-ciberataque-compromete-datos-miles-clientes-electricidad-gas.html
[21] https://thehackernews.com/2025/05/over-70-malicious-npm-and-vs-code.html
[22] https://www.sonatype.com/hubfs/White_Papers/How-North-Korea-Backed-Lazarus-Group-is-Weaponizing-Open-Source-Whitepaper.pdf
[23] https://socket.dev/blog/north-korean-apt-lazarus-targets-developers-with-malicious-npm-package
[24] https://socket.dev/blog/lazarus-strikes-npm-again-with-a-new-wave-of-malicious-packages
[25] https://blog.gitguardian.com/the-state-of-secrets-sprawl-2025/
[26] https://www.cyberhaven.com/blog/cyberhavens-chrome-extension-security-incident-and-what-were-doing-about-it
[27] https://www.darktrace.com/fr/blog/cyberhaven-supply-chain-attack-exploiting-browser-extensions
[28] https://www.malwarebytes.com/blog/news/2025/01/google-chrome-ai-extensions-deliver-info-stealing-malware-in-broad-attack
[29] https://blog.sekoia.io/targeted-supply-chain-attack-against-chrome-browser-extensions/
[30] https://research.checkpoint.com/2024/rafel-rat-android-malware-from-espionage-to-ransomware-operations/
[31] https://www.cleafy.com/cleafy-labs/medusa-reborn-a-new-compact-variant-discovered
[32] https://www.cleafy.com/cleafy-labs/bingomod-the-new-android-rat-that-steals-money-and-wipes-data
[33] https://www.lookout.com/threat-intelligence/article/lookout-discovers-new-spyware-by-north-korean-apt37
[34] https://www.lookout.com/threat-intelligence/article/eaglemsgspy-chinese-android-surveillanceware
[35] https://cloud.google.com/blog/topics/threat-intelligence/russia-targeting-signal-messenger

leveraging of Signal, as part of a recent spearphishing campaign conducted by CozyLarch UTA0304, UTA0307 and Storm-2372[36].

In October 2024, Qualcomm published a **vulnerability impacting its Qualcomm's Digital Signal Processor (DSP)** software[37]. The vulnerability has an impact on chipsets widely used by various mobile devices and was reported to have been exploited in the wild[38].

In 2025, iVerify published an in-depth technical report revealing that state-linked telecommunications providers continue to **exploit vulnerabilities in outdated mobile signalling protocols—specifically SS7 and Diameter**[39]. These protocols, which underpin global mobile communications, were not designed with encryption or strong authentication, leaving them susceptible to interception, location tracking and session hijacking. iVerify demonstrated that operators with privileged access to international telecom infrastructure—such as China Mobile International and China Telecom Global—can remotely monitor and manipulate mobile communications across borders without needing access to the target's device. These operations are silent, infrastructure-level and difficult to detect, posing significant risks to diplomats, journalists, and political actors.

4.4 THREAT GROUPS CONVERGING

Across the period, the lines between hacktivism, cybercrime and state-nexus activity continued to blur. Intrusion sets historically distinguished by TTPs' level of advancement. conducted activities, or assessed objectives increasingly shared toolsets and modus operandi.

This was notably exemplified by hacktivist-led DDoS waves by pro-Russia groups around electoral events, where increased activity was often observed as typical FIMI-aligned behaviour to associate disruption with aspects of information operations. A prominent facet of this trend is **faketivism**, where state-aligned intrusion sets leverage hacktivist personas and activities. Notable examples include Cyber Army of Russia Reborn, associated to Russia-nexus Sandworm[40], and the CyberAv3ngers group linked to Iran's IRGC[41].

In parallel, **hacktivist tooling and criminal ecosystems increasingly intersect**. FunkSec's emergence in late 2024 brought FunkLocker ransomware, blending political messaging with financial extortion, underscoring how quickly ideology-driven branding can pivot to monetisation[42] [43]. Hacktivists, seeking funding and visibility, embraced ransomware beyond DDoS and defacements. CyberVolk, operating in line with Russian interests, has used and promoted multiple strains—AzzaSec, HexaLocker, Parano, as well as LockBit and Chaos—since May 2024[44] [45] [46]. KillSec, originally a pro-Russia hacktivist brand aligned with Anonymous, debuted its platform in June 2024[47].

Another aspect of this trend is the **false-flag operation** carried out by Turla, taking over Transparent Tribe's infrastructure[48] [49], or **cybercriminals masquerading as other cybercriminal groups** or spoofing their brand, as notably seen with email extortion campaigns impersonating the CL0P ransomware group[50], physical

[36] https://www.volexity.com/blog/2025/02/13/multiple-russian-threat-actors-targeting-microsoft-device-code-authentication/
[37] https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html
[38] https://securitylab.amnesty.org/latest/2024/12/a-digital-prison-surveillance-and-the-suppression-of-civil-society-in-serbia/
[39] https://iverify.io/blog/abusing-data-in-the-middle-surveillance-risks-in-china-s-state-owned-mobile-ecosystem
[40] https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm
[41] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a
[42] https://research.checkpoint.com/2025/funksec-alleged-top-ransomware-group-powered-by-ai/
[43] https://therecord.media/funksec-ransomware-using-ai-malware
[44] https://www.rapid7.com/blog/post/2024/10/03/ransomware-groups-demystified-cybervolk-ransomware/
[45] https://detect.fyi/cybervolks-ransomware-ad38134b1b0a
[46] https://www.sentinelone.com/labs/cybervolk-a-deep-dive-into-the-hacktivists-tools-and-ransomware-fueling-pro-russian-cyber-attacks/
[47] https://thecyberexpress.com/killsec-launches-raas-program/
[48] https://www.microsoft.com/en-us/security/blog/2024/12/04/frequent-freeloader-part-i-secret-blizzard-compromising-storm-0156-infrastructure-for-espionage/
[49] https://blog.lumen.com/snowblind-the-invisible-hand-of-secret-blizzard/
[50] https://www.barracuda.com/company/news/2025/fraudsters-impersonate-clop-ransomware-to-extort-businesses

ransom letters mailed to executives by criminals masquerading as the BianLian ransomware group[51], or the preposterous re-emergence of Babuk ransomware[52] [53].

State-nexus intrusion sets also leveraged or brokered cybercrime tradecraft, as illustrated by DPRK-nexus Kimsuky using the Clickfix technique, Andariel linked to the Play ransomware activity, likely as an affiliate or IAB, and Moonstone Sleet reported leveraging the Qilin ransomware[54] . Similar cross-over was identified with China-nexus intrusion sets, with NailoLocker operations in June and October 2024 targeting the EU health sector, and Mustang Panda leveraging the RA ransomware, plausibly in the frame of moonlighting activities[55] [56]. State-nexus intrusion sets were increasingly reported leveraging cybercriminal infrastructure. APT29 and Sandworm were observed using commercial residential proxy networks and sharing hosting with cybercriminals—while Andariel[57] and Sandworm[58] were seen deploying commodity infostealers. Conversely, **cybercriminal groups adopted social engineering techniques seen used by state-nexus groups**, as observed with FIN6 leveraging job applications and fabricated LinkedIn personas to deliver malware, echoing DPRK's playbook[59].

Finally, **hybrid campaigns** should also be mentioned in this section, especially with activities aligned with Russian objectives continuing to impact EU MSs beyond cyberspace[60] [61]. In November 2024, Romania's Constitutional Court annulled the presidential first-round results after its intelligence agencies presented declassified findings that Russian-linked cyber operations—including coordinated social media campaigns with AI-driven misinformation and alleged cyberattacks—distorted the electoral process in favour of the far-right candidate[62]. In March 2025, investigative reporting detailed pro-Russia groups using Telegram to recruit EU-based individuals for sabotage, vandalism, arson and influence operations across NATO countries[63] [64] [65] [66] [67] [68].

4.5 PREDICTABLE USE OF AI

Over the reporting period, the **continuous use of AI across multiple intrusion sets** continued to be observed, **both as tools** to facilitate or enhance offensive activities and as **targets** for exploitation. The large-scale deployment and availability of AI systems objectively generate a new level of scalability in malicious activity on the side of attackers[69]. While AI-enabled threat activity previously involved attempts by threat actors to use consumer-grade AI tools to augment existing operations, rather than achieve breakthrough capabilities, the emergence of stand-alone malicious AI systems since the beginning of 2025 is of particular concern.

As a predictable trend, Large Language Models **(LLMs) are leveraged to craft more convincing phishing emails**; with reportedly over 80% of all phishing emails identified between September 2024 and February 2025 using AI to some extent[70]. AI is notably used in vishing and online fraud involving impersonation, with the

[51] https://www.ic3.gov/psa/2025/psa250306-2
[52] https://www.rapid7.com/blog/post/2025/04/02/a-rebirth-of-a-cursed-existence-the-babuk-locker-2-0/
[53] https://www.lexmark.com/en_us/solutions/security/lexmark-security-advisories/current-advisories/babuk2-incident-notice.html
[54] https://www.linkedin.com/posts/microsoft-threat-intelligence_since-late-february-2025-microsoft-has-observed-activity-7303505954291994624-1W2t
[55] https://www.security.com/threat-intelligence/chinese-espionage-ransomware
[56] https://unit42.paloaltonetworks.com/ra-world-ransomware-group-updates-tool-set/
[57] https://www.infostealers.com/article/meet-the-top-5-threat-actors-exploiting-infostealers-data-to-breach-companies/
[58] https://www.virusbulletin.com/uploads/pdf/conference/vb2023/papers/Infostealers-investigate-the-cybercrime-threat-in-its-ecosystem.pdf
[59] https://therecord.media/fin6-recruitment-scam-malware-campaign
[60] https://www.polskieradio.pl/395/7784/Artykul/3422946,poland-thwarts-belarusian-and-russian-sabotage-network
[61] https://csds.vub.be/publication/shadow-war-what-estonia-and-poland-tell-us-about-russias-clandestine-operations-in-europe/
[62] https://www.ccr.ro/comunicat-de-presa-6-decembrie-2024/
[63] https://telex.hu/belfold/2025/01/23/tobb-magyarorszagi-iskolaban-is-bombariado-van
[64] https://www.dnevnik.si/novice/kronika/zaradi-groznje-evakuirali-vec-slovenskih-sol-2714086/
[65] https://www.zurnal24.si/slovenija/slovenski-student-vdrl-v-postni-nabiralnik-rusa-ki-je-vceraj-solam-posiljal-groznje-435943
[66] https://www.sk-cert.sk/sk/varovanie-pred-zvysenym-rizikom-kybernetickych-bezpecnostnych-utokov-2/index.html
[67] https://stolica.bg/sofia/nad-10-stolichni-uchilishta-sa-poluchili-zaplashitelni-imeili
[68] https://investigations.news-exchange.ebu.ch/playing-with-fire-are-russias-hybrid-attacks-the-new-european-war/
[69] https://www.group-ib.com/blog/the-dark-side-of-automation-and-rise-of-ai-agent/
[70] https://www.knowbe4.com/hubfs/Phishing-Threat-Trends-2025_Report.pdf?hsLang=en

use of deepfakes[71] [72] [73] [74] [75] [76] [77], as well as for malware development[78] [79] [80] [81]. Threat groups were observed to be leveraging commercial LLMs to augment operations, as well as jailbroken or retrained (diverted) LLMs such as WormGPT, EscapeGPT and FraudGPT, to **automate social engineering activities** and accelerate the development of malicious tools[82] [83]. China-nexus, Iran-nexus and DPRK-nexus intrusion sets were reported using AI solutions, including Google's Gemini[84] and OpenAI's ChatGPT[85], primarily as research assistants for boosting productivity as well as for reconnaissance and anomaly detection evasion. Famous Chollima was notably seen using AI to generate convincing LinkedIn profiles and support communications with victim organisations[86] [87] [88]. The emergence of allegedly **stand-alone malicious AI systems** over the past two quarters, such as Xanthorox AI, likely indicates a trend of threat groups moving beyond jailbreaks towards customised tools running on local servers to avoid detection[89].

Another noteworthy trend is the **use of AI as a lure**, in the context of the rising popularity of generative AI. Multiple sources reported the proliferation of fraudulent websites, impersonating legitimate AI tools such as Kling AI, Luma AI, Canva Dream Lab and DeepSeek-R1, to deliver malware[90] [91] [92] [93] [94] [95]. Further reporting included the deployment of ransomware and malware masquerading as legitimate AI tool installers[96].

Also observed was the **targeting of the AI supply chain**, with poisoned hosted machine learning (ML) models and Python Package Indexes (PyPI) reportedly used to distribute trojanised packages[97], and a supply chain attack vector called 'Rules File Backdoor', enabling the injection of malicious instructions into configuration files that AI coding assistants use, like Cursor and GitHub Copilot[98]. Interestingly, and as generative AI becomes increasingly integrated into software development, the term 'slopsquatting' was introduced[99]. Although publicly available evidence suggests that misuse of LLMs and other AI tools occurs more frequently than direct efforts to **compromise AI systems**, researchers identified multiple Proofs of Concept (PoC) by which an intrusion set could subvert the intended function of AI models for malicious purposes[100]. The increased integration of AI systems into enterprise environments introduces a potentially vulnerable **new attack surface**. AI software is not immune to vulnerabilities, as exemplified by the critical remote code execution vulnerability discovered in Langflow or Microsoft 365 Copilot[101]. The **infrastructure on which AI systems rely** to operate has also been found vulnerable, for instance through CVE-2024-27564, a Server-Side Request Forgery vulnerability present in commit f9f4bbc, used within OpenAI's ChatGPT system[102].

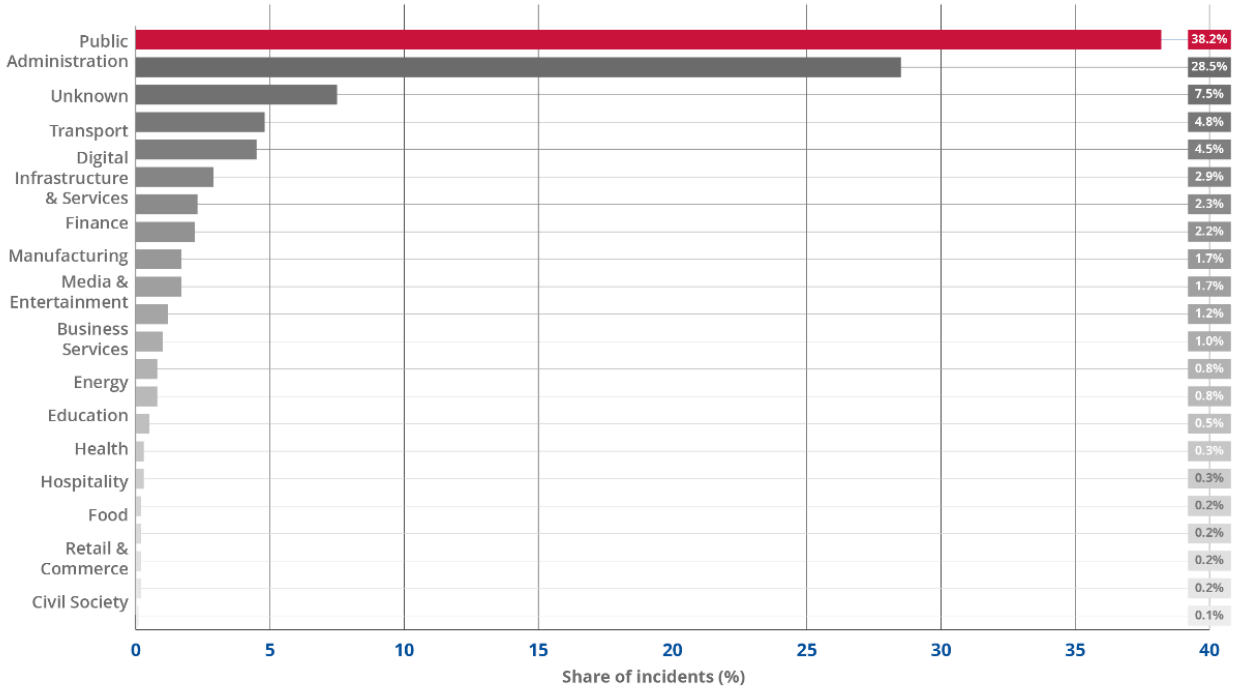
[71] https://www.trendmicro.com/vinfo/gb/security/news/cybercrime-and-digital-threats/surging-hype-an-update-on-the-rising-abuse-of-genAI
[72] https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk
[73] https://www.chainalysis.com/blog/2024-pig-butchering-scam-revenue-grows-yoy/
[74]https://www.sentinelone.com/labs/akirabot-ai-powered-bot-bypasses-captchas-spams-websites-at-scale/
[75] https://www.trendmicro.com/en_us/research/25/c/ai-assisted-fake-github-repositories.html
[76] https://www.phonely.ai/blogs/how-does-ai-voice-cloning-work
[77] https://www.europol.europa.eu/cms/sites/default/files/documents/vishing_final_version.pdf
[78] https://www.security.com/threat-intelligence/malware-ai-llm
[79] https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta547-targets-german-organizations-rhadamanthys-stealer
[80] https://research.checkpoint.com/2025/funksec-alleged-top-ransomware-group-powered-by-ai/
[81] https://www.sentinelone.com/blog/blackmamba-chatgpt-polymorphic-malware-a-case-of-scareware-or-a-wake-up-call-for-cyber-security/
[82] https://www.trendmicro.com/vinfo/gb/security/news/cybercrime-and-digital-threats/back-to-the-hype-an-update-on-how-cybercriminals-are-using-genAI
[83] https://blogs.microsoft.com/on-the-issues/2025/02/27/disrupting-cybercrime-abusing-gen-ai/
[84] https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai
[85] https://openai.com/global-affairs/disrupting-malicious-uses-of-ai/
[86] https://securityboulevard.com/2025/04/north-korean-group-creates-fake-crypto-firms-in-job-complex-scam/
[87] https://unit42.paloaltonetworks.com/north-korean-synthetic-identity-creation/
[88] https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us
[89] https://destcert.com/resources/xanthorox-ai/
[90] https://www.morphisec.com/blog/new-noodlophile-stealer-fake-ai-video-generation-platforms/
[91] https://research.checkpoint.com/2025/impersonated-kling-ai-site-installs-malware/
[92] https://cloud.google.com/blog/topics/threat-intelligence/cybercriminals-weaponize-fake-ai-websites
[93] https://securelist.com/browservenom-mimicks-deepseek-to-use-malicious-proxy/115728/
[94] https://labs.k7computing.com/index.php/android-banking-trojan-octov2-masquerading-as-deepseek-ai/
[95] https://www.malwarebytes.com/blog/news/2025/03/deepseek-users-targeted-with-fake-sponsored-google-ads-that-deliver-malware
[96] https://blog.talosintelligence.com/fake-ai-tool-installers/
[97] https://www.reversinglabs.com/blog/malicious-attack-method-on-hosted-ml-models-now-targets-pypi
[98] https://www.pillar.security/blog/new-vulnerability-in-github-copilot-and-cursor-how-hackers-can-weaponize-code-agents
[99] https://socket.dev/blog/slopsquatting-how-ai-hallucinations-are-fueling-a-new-class-of-supply-chain-attacks
[100] https://arxiv.org/pdf/2406.13843
[101] https://www.aim.security/lp/aim-labs-echoleak-blogpost
[102] https://veriti.ai/blog/veriti-research/cve-2024-27564-actively-exploited/

5. SECTORIAL ANALYSIS

This section examines cyber threats from a sectorial perspective. While it includes the 18 sectors identified under the NIS2 Directive as high-criticality or other critical, our analysis extends beyond these to consider a broader range of sectors. In our analysis, particular emphasis is placed on the five most targeted sectors to highlight key threat patterns.

Over the reporting period, ENISA collected and curated 4 875 events. **28.5% of the total number of incidents were not associated to a specific sector**, either because the sector was not properly documented (i.e., private sector, private companies) or not mentioned at all. Once this significant share is redacted, the top five targeted sectors in the EU include **public administration** (38.2%), **transport** (7.5%), **digital infrastructure and services** (4.8%), **finance** (4.5%) and **manufacturing** (2.9%). While recorded incidents include non-NIS2 sectors, the close alignment of the top five targeted sectors with sectors explicitly covered under the directive confirms the relevance of the NIS2 approach[103], as **essential entities represent 53.7% of the total number of recorded incidents.**

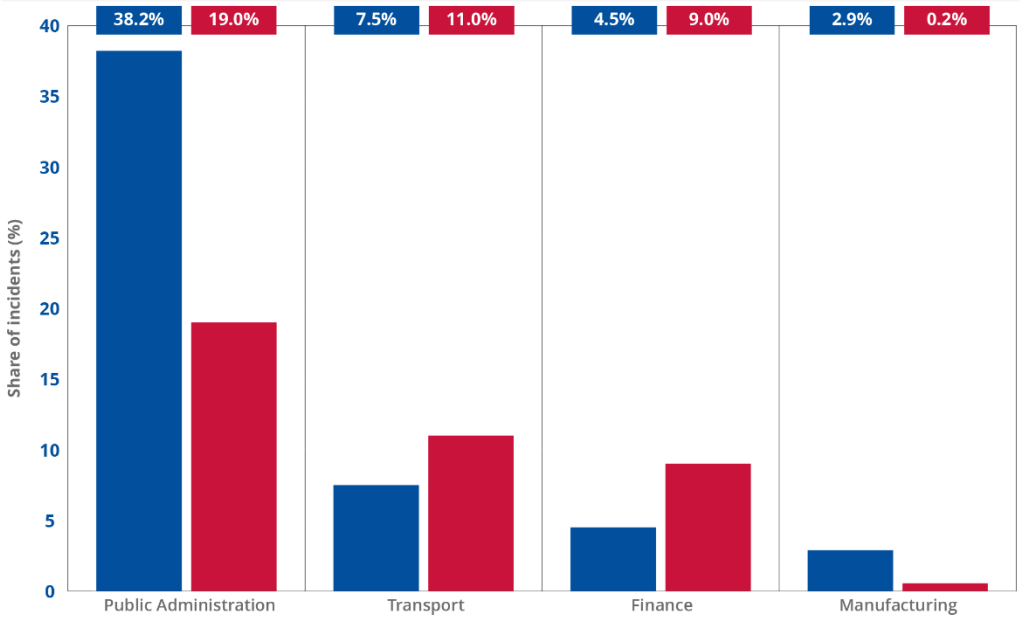
Fig. 7 - Share of recorded incidents by sector.
Source: ENISA dataset



While public administration, transport and finance were already listed as the top targeted sectors of EU MSs in the previous reporting period, incidents targeting public administration substantially increased, notably due to the increase of hacktivist-led DDoS attacks against this sector. Overall, **DDoS attacks were the most prevalent threat and affected multiple sectors in the EU** (81.4%).

[103] https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

Fig. 8 - Comparison of incident shares by sector - **ETL 2025** vs. **ETL 2024**.
Source: ENISA dataset

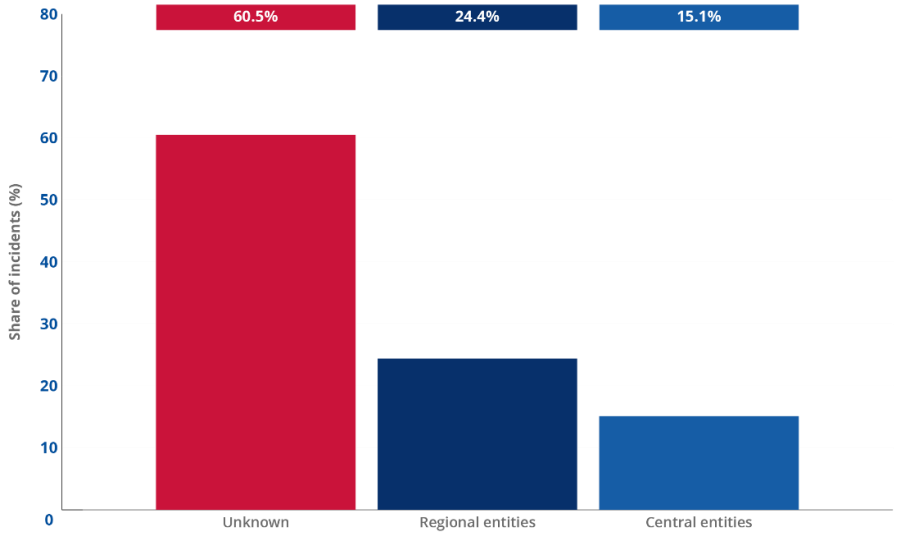


5.1 PUBLIC ADMINISTRATION

As in the previous ETL, public administration remains the most targeted sector (38%), showing a significant increase, primarily due to hacktivist-led DDoS attacks. The highest number of recorded incidents reportedly impacted the public administration sector in France (27%), Italy (26.3%) and Germany (16.2%), followed by Spain (15.3%) and Poland (15.1%).

The distribution of incidents affecting public administration over the reporting period shows that **incidents primarily impacted regional** (24.4 %) and **central entities** (15.1%).

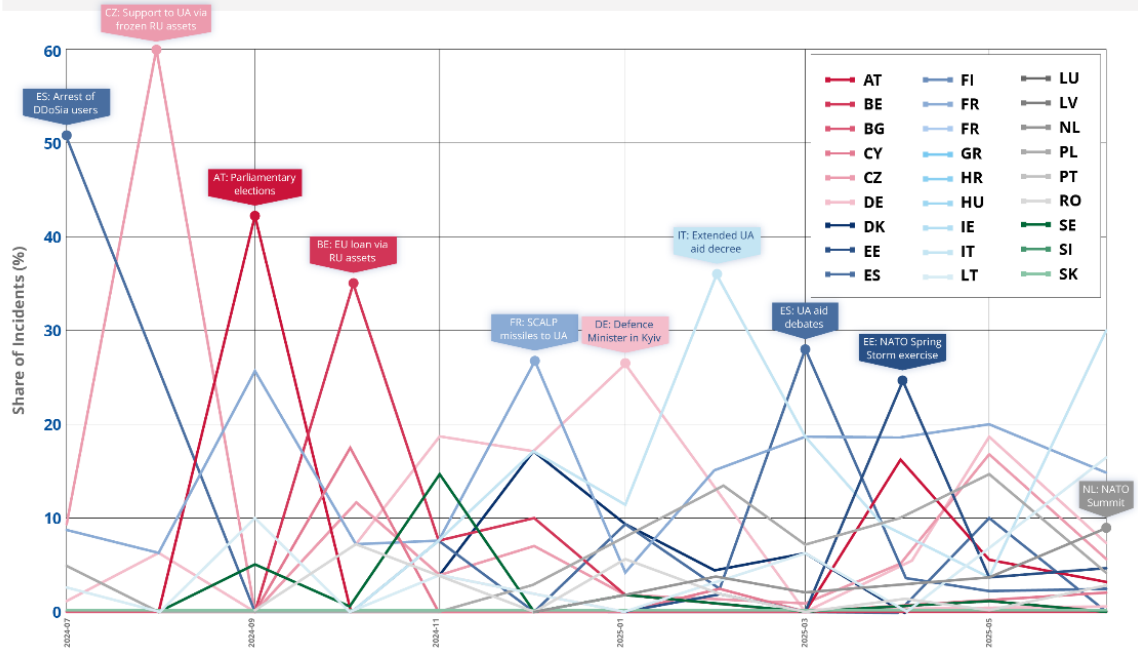
Fig. 9 - Distribution of incident against the EU public administration.
Source: ENISA dataset



Within the central entities category, defence and military related entities and intelligence and security services represented 2.4%, while law enforcement related bodies made up 0.9% and political parties represented around 0.1%. Diplomatic missions such as embassies accounted for 1.4%. Union entities and NATO Enterprise each contributed 0.7% of all incidents. 1% of recorded DDoS attacks targeting the websites of EU organisations were related to non-EU countries, namely Iranian or Israeli organisations.

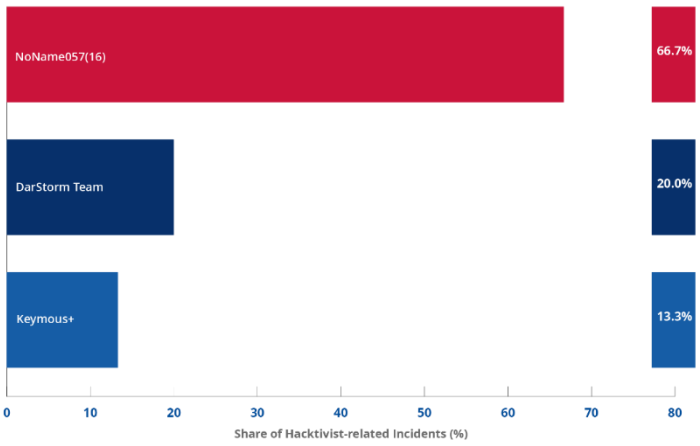
Unsurprisingly, this threat picture is **largely impacted by hacktivist-led DDoS (96.2%) attacks**, with the targeting of public administration websites being the **first-line option around specific events**, such as takedowns and arrests, electoral processes or high visibility events[104], as illustrated with a few contextualised examples hereunder.

Fig. 10 - Contextualised DDoS against the EU public administration.
Source: ENISA



Hacktivist groups NoName057(16) (66.7%), Dark Storm (20%), and Keymous+ (13.3%) were the most active intrusion sets targeting public administration in the EU. Alliances such as 7 October Union and Holy League contributed to the increasing tempo and intensity of DDoS attacks targeting the websites and portals of public administrations in EU MSs, in the context of Russia's war of aggression against Ukraine, as well as the Israel-Hamas conflict. Other claims made by these alliances also pertained to societal issues, including EU migration policies, LGBTQ+ legislation, or perceived anti-religious stances.

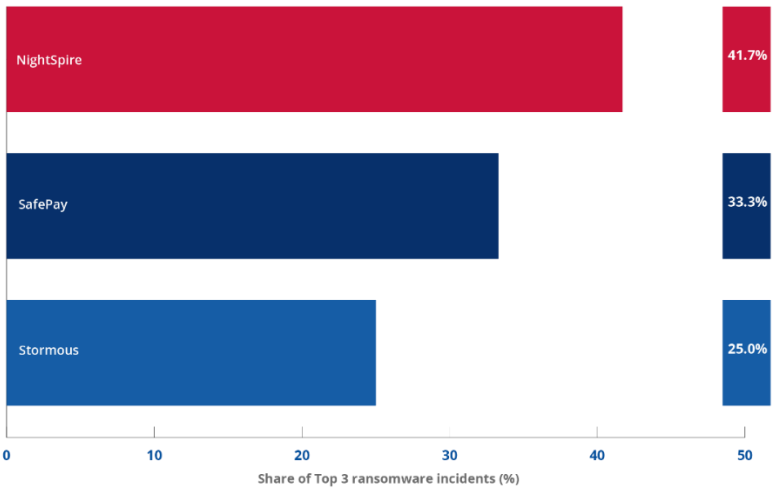
Fig. 11 - Top 3 hacktivist groups targeting the EU public administration.
Source: ENISA dataset



[104] https://therecord.media/austria-websites-ddos-incidents-pro-russia-hacktivists

The EU public administration sector continued facing ransomware incidents (2.2%), which were particularly prevalent against **municipalities**. The most reported strains used against the public administration sector included NightSpire (41.7%), SafePay (33.3%), and Stormous (25%) ransomware. While accounting for 26 events against the EU's public administration sector in the last ETL iteration, the LockBit ransomware was not seen to be active over this reporting period, highly likely as a consequence of law enforcement's Operation Cronos in February 2024[105]. Data breaches relevant to the EU public administration accounted for 17% of all recorded data breaches.

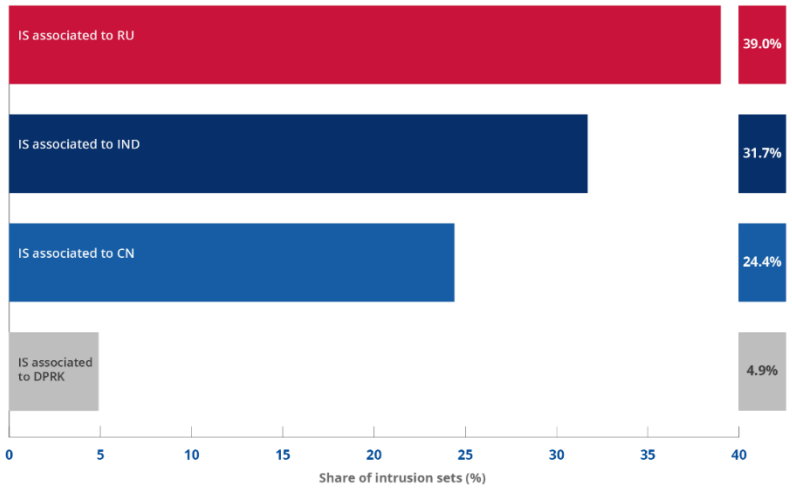
Fig. 12 - Top 3 ransomware claims against the EU public administration.
Source: ENISA dataset



Overall, the targeting of the public administration by State-nexus intrusion sets underscores a focus on diplomatic, and governmental entities, with Russia-nexus and China-nexus offensive cyber activities displaying the broadest sectorial spread, and India-nexus activity showing a clear unique focus on this sector. With a total of 77 incidents, and excluding unidentified sectorial targeting, **public administration was the most targeted sector by state-nexus intrusion sets in the EU, for cyberespionage purposes**.

China-nexus intrusion sets including **APT31, Mustang Panda**, and **APT17** notably focused on government entities across several EU member states including ministries of foreign affairs and municipal administrations.

Fig. 13 - Targeting of EU public administration by state-aligned groups
Source: ENISA dataset



[105] https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

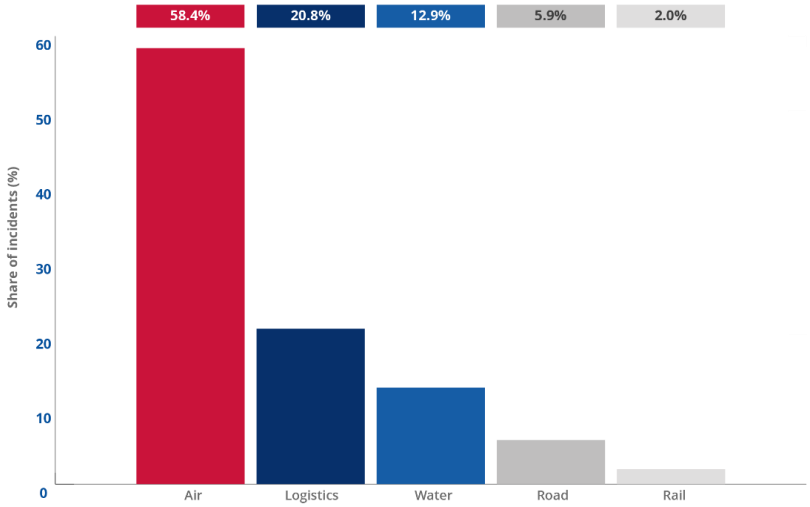
The targeting of the public administration by Russia-nexus threat groups such as **APT28, APT29, Turla,** and **GoldenJackal**, is more diverse, impacting diplomatic entities, ministries, law enforcement and political parties, in addition to core government institutions. A newcomer among the most active state-nexus intrusion sets in the EU, **Sidewinder** demonstrated a clear focus on diplomatic entities and governmental organisations within EU public administrations.

5.2 TRANSPORT

While remaining in second position compared to the previous ETL, the number of recorded incidents against the EU transport sector amounted to 7.5% of all incidents across all sectors. Of note, 12% of the incidents with a significant impact reported under the NIS directive in 2024 were incidents in the transport sector[106].

The distribution of incidents impacting the transport sector in the EU highlights a concentration of incidents in air transport (58.4%), followed by logistics (20.8%). Of note, it is likely logistics would include entities involved in air, water, road and rail transport.

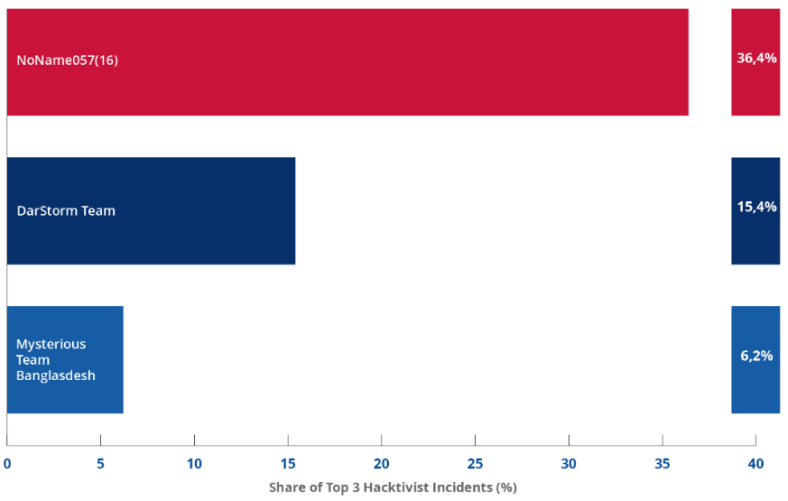
Fig. 14 - Distribution of incidents against the EU transport sector.
Source: ENISA dataset



Yet again, the transport sector was **largely impacted by hacktivist-led DDoS attacks (87.6%);** the most active hacktivist groups against this sector included NoName057(16) (36.4%), DarkStorm Team (15.4%) and Mysterious Team Bangladesh (6.2%).

As previously mentioned, increased activity was **triggered by specific events at the EU national level**[107] [108] [109] **and/or support for Ukraine**.

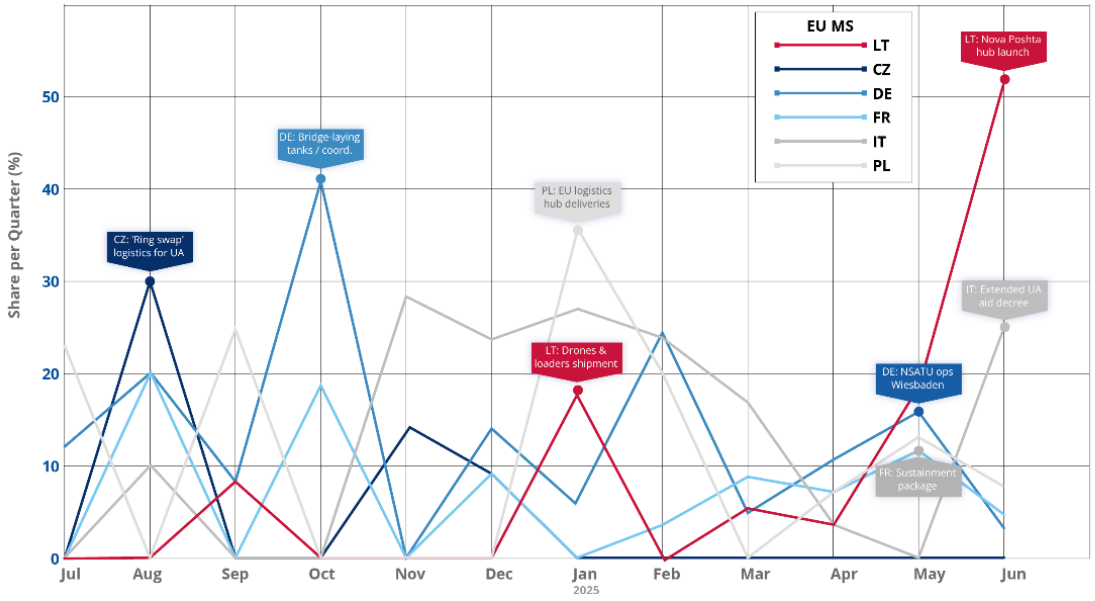
Fig. 15 - Top 3 hacktivist groups targeting the EU transport sector
Source: ENISA dataset



[106] https://ciras.enisa.europa.eu/ciras-consolidated-reporting
[107] hxxps://t.me/Darkstormbackup2
[108] hxxps://t.me/NNM05716_en_vers/71
[109] hxxps://t.me/+uIR_0146Ndk1NTUy

This is notably illustrated by NoName057(16) explicitly mentioning announcements by Czechia, Latvia and Poland related to new bilateral security agreements with Ukraine as a trigger to target transport entities in these EU MSs[110] [111] [112]. In December 2024, Italy's Malpensa and Linate airport portals were briefly unreachable in attacks later claimed by NoName057(16)[113] [114] [115], likely in the context of Italy's government decree to authorise the transfer of means, materials and equipment to Ukraine .

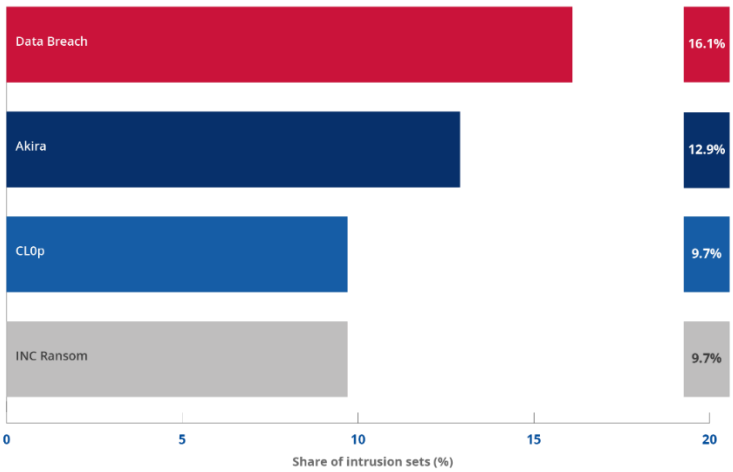
Fig. 16 - Contextualised DDoS against the EU transport sector.
Source: ENISA



Cybercrime incidents against the transport sector accounted for 8.4% of all incidents, with ransomware accounting for 83.9% and data breaches 16.1% of cybercrime incidents.

Top three ransomware claims against the EU transport sector include Akira (12.9%), INC Ransom (9.7%), and Cl0p (9,7%). Despite being a small share of recorded events, ransomware displayed a more disruptive impact in a few cases. For instance, following an incident reportedly involving Akira ransomware, the Split Airport in Croatia saw the disruption of the passenger reception information system, ultimately impacting the landing and take-off of aircrafts and leading to a temporary suspension of all flights[116] [117].

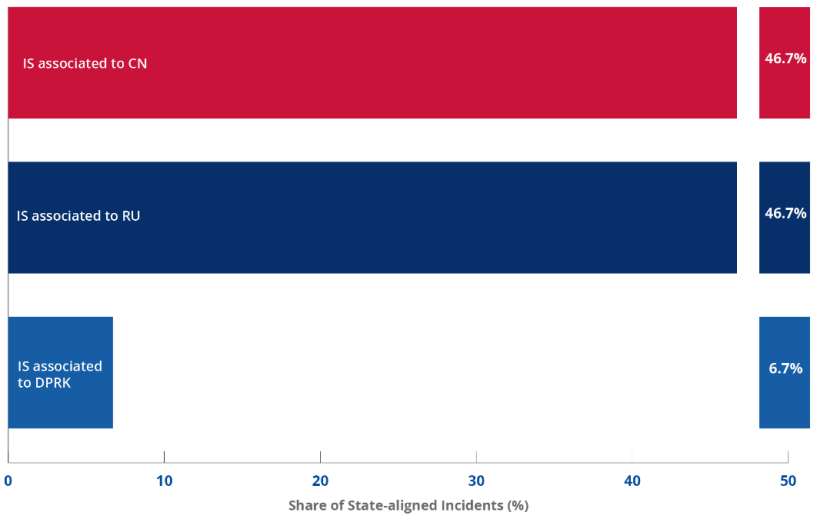
Fig. 17 - Cybercrime claims against the EU transport sector.
Source: ENISA dataset



[110] https://t.me/noname05716eng/3677
[111] https://t.me/noname05716eng/3927, https://t.me/noname05716/8458
[112] https://t.me/noname05716/8917
[113] https://www.reuters.com/technology/cybersecurity/cyber-attack-italys-foreign-ministry-airports-claimed-by-pro-russian-hacker-2024-12-28/
[114] https://www.dw.com/en/pro-russian-hackers-target-italian-airport-websites/a-71176385
[115] https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.codiceRedazionale=25A03003&atto.dataPubblicazioneGazzetta=2025-05-20
[116] https://glashrvatske.hrt.hr/en/domestic/split-airport-after-the-hacker-attack-we-will-not-negotiate-11673909
[117] https://www.exyuaviation.com/2024/07/split-airport-hacked-by-akira-ransomware.html

While low overall (4.1%), the **targeting of the EU transport sector by state-nexus threat groups was dominated by China-nexus and Russia-nexus intrusion sets** (46.7%). China-nexus intrusion sets, including Mustang Panda, UNC5221 and APT41, notably focused on maritime and shipping and logistics subsectors across multiple EU MSs. This activity aligns with Beijing' strategic interest in securing maritime supply chains and transport corridors tied to the Belt and Road Initiative, as well as maintaining visibility over European trade infrastructure. Russia-nexus intrusion sets, notably APT28, seemingly focused on air transport, logistics and freight, particularly in Germany, France and Belgium, likely reflecting Moscow's broader strategy to target the critical infrastructure of NATO Allies, especially in the context of the war in Ukraine.

Fig. 18 - State-aligned activities against the EU transport sector.
Source: ENISA dataset

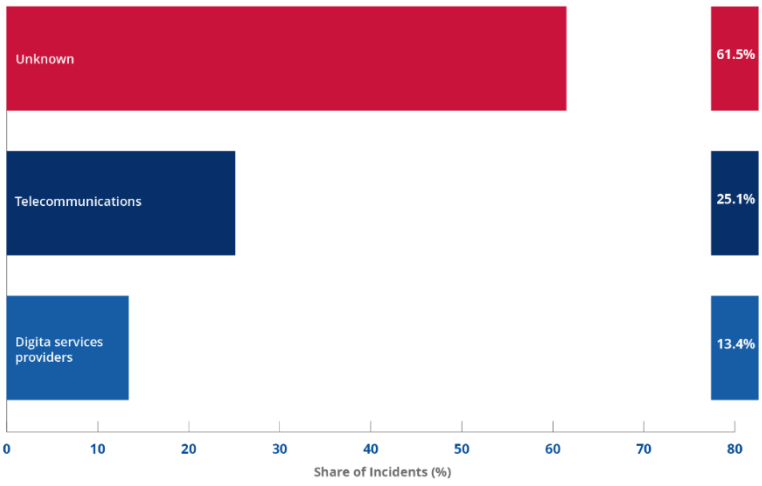


Smaller shares are associated to **DPRK-nexus** Lazarus (6.7%), possibly aiming at gathering strategic data pertaining to the evasion of sanctions. Rare Werewolf's activity against logistics of an EU MS represent a residual threat, likely linked to spill over activities.

5.3 DIGITAL INFRASTRUCTURE AND SERVICES

For the purpose of this report, the notion of digital infrastructure and services (DIS) includes the digital infrastructure sector in accordance with NIS2, as well as incidents related to digital providers and ICT service management. With a share of 4.8% of overall incidents, DIS comes third in the top five targeted sectors across the EU over the reporting period. While the targeting of DIS likely stems from the sector being of high value for collecting data and disrupting services at a larger scale, it is likely this also speaks to the dispersed nature and heterogeneous levels of maturity of the organisations comprising this ecosystem.

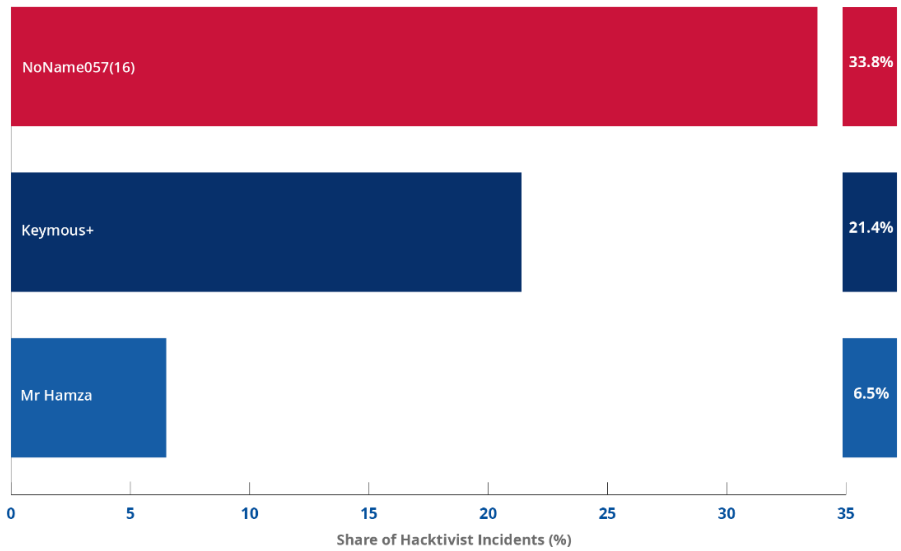
Fig. 19 - Distribution of incidents against EU Digital Infrastructure & Services
Source: ENISA dataset



Among DIS entities, the most impacted sub-sectors include telecommunications (25.1%), and digital services providers (DSP) (13.4%).

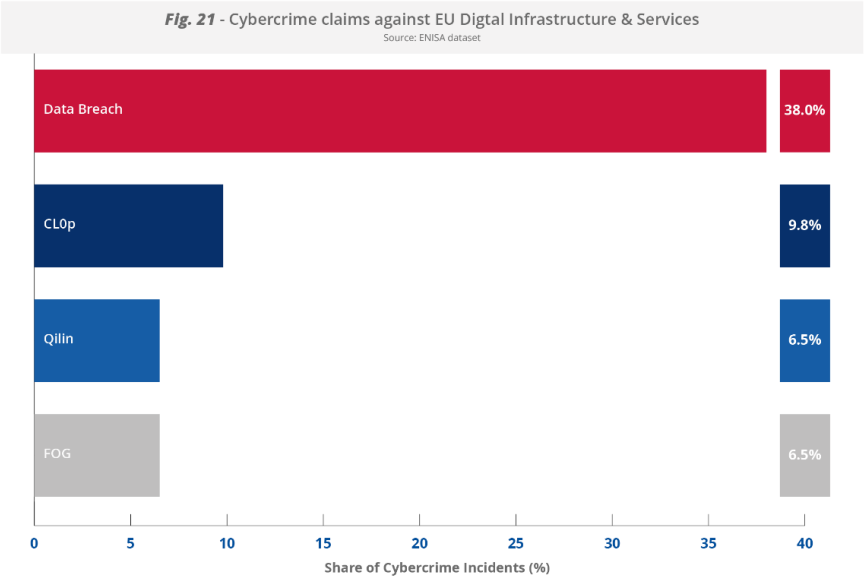
Hacktivist-led DDoS attacks against DIS websites accounted for 57.5% of attacks on EU DIS, with NoName057(16) (33.8%), Keymous+ (21.4%) and Mr Hamza (6.5%) reportedly the most active groups.

Fig. 20 - Top 3 hacktivist claims against EU Digital Insfrastructure & Services
Source: ENISA dataset



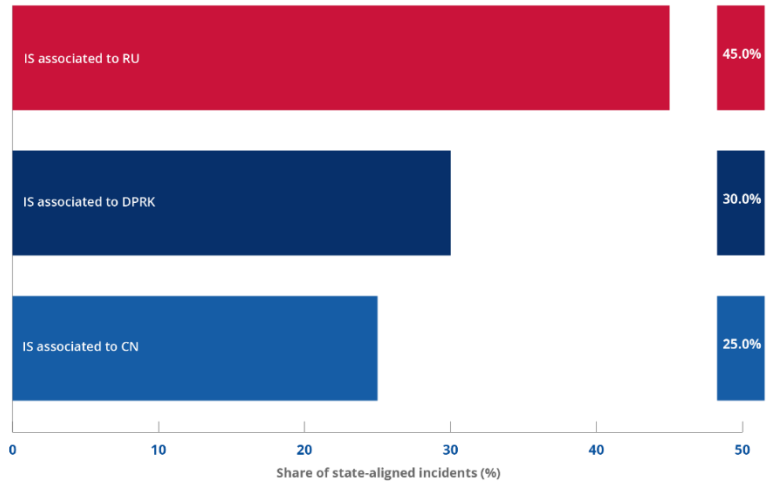
Representing 34.3% of overall incidents, the cybercrime threat to EU DIS includes data breaches (38%) and the deployment of Cl0p (9.8%), FOG, and Qilin (6.5%). It is highly likely DIS is perceived as a target of interest due to the amount and criticality of data they hold, as well as the opportunity to disrupt services across a large number of organisations, sectors and EU MSs, increasing the likelihood of ransom demands being met.

Fig. 21 - Cybercrime claims against EU Digtal Infrastructure & Services
Source: ENISA dataset



With a total share of incidents amounting to 8.2%, targeting DIS in the EU shows a clear concentration of a few key intrusion sets, notably a stark dominance of operations linked to Russia-nexus intrusion sets, primarily driven by APT29[118] and APT28. These intrusion sets account for the majority of observed incidents, with campaigns targeting IT service providers and telecommunications companies. DPRK-nexus malicious activities against this sector are largely skewed by Famous Chollima's activities targeting IT providers and software developers in the EU[119] [120] , and the DeceptiveDevelopment campaign targeting freelance software developers[121] [122]. In contrast, activity associated to China-nexus intrusion sets, notably Salt Typhoon, appears less frequently but concentrates on telecommunications infrastructure, with long running highly advanced campaigns, consistent with the broader global patterns of China-nexus cyberespionage[123] [124] [125] [126] [127].

Fig. 22 - State-aligned activities against EU Digital Infrastructure & Services
Source: ENISA dataset



[118] https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/
[119] https://go.crowdstrike.com/2025-global-threat-report.html
[120] https://go.recordedfuture.com/hubfs/reports/cta-nk-2025-0213.pdf
[121] https://securityscorecard.com/blog/operation-99-north-koreas-cyber-assault-on-software-developers/
[122] https://www.securonix.com/blog/research-update-threat-actors-behind-the-devpopper-campaign-have-retooled-and-are-continuing-to-target-software-developers-via-social-engineering/
[123] https://go.recordedfuture.com/hubfs/reports/cta-cn-2025-0213.pdf
[124] https://blog.talosintelligence.com/salt-typhoon-analysis/
[125] https://www.sentinelone.com/labs/operation-digital-eye-chinese-apt-compromises-critical-digital-infrastructure-via-visual-studio-code-tunnels/
[126] https://blog.eclecticiq.com/china-nexus-threat-actor-actively-exploiting-ivanti-endpoint-manager-mobile-cve-2025-4428-vulnerability
[127] https://www.europarl.europa.eu/doceo/document/E-10-2025-002101_EN.html

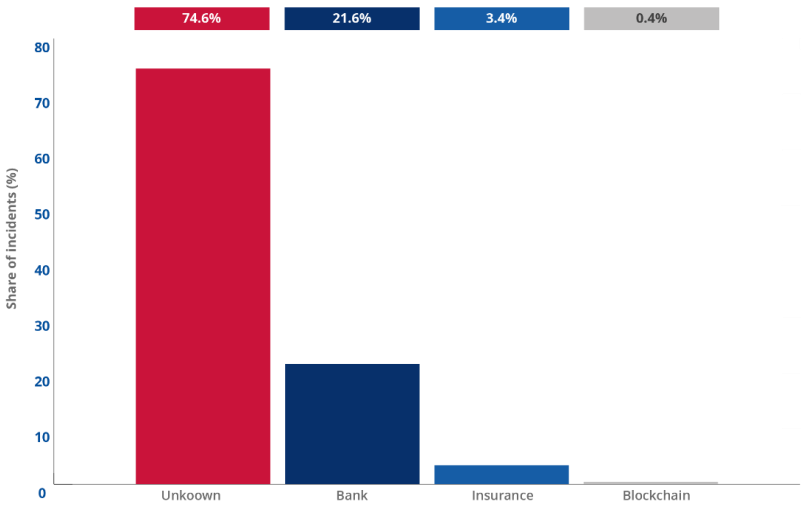
5.4 FINANCE

The finance sector accounted for 4.7 % of all collected incidents, with hacktivist-led DDoS attacks clearly dominating the threat picture, making up 83.5% of the incidents, followed by cybercrime (14.8%) and state-aligned (1.7%).

Of note 11% of the incidents with a significant impact reported under the network and information security (NIS) directive in 2024 were incidents in the finance sector[128].

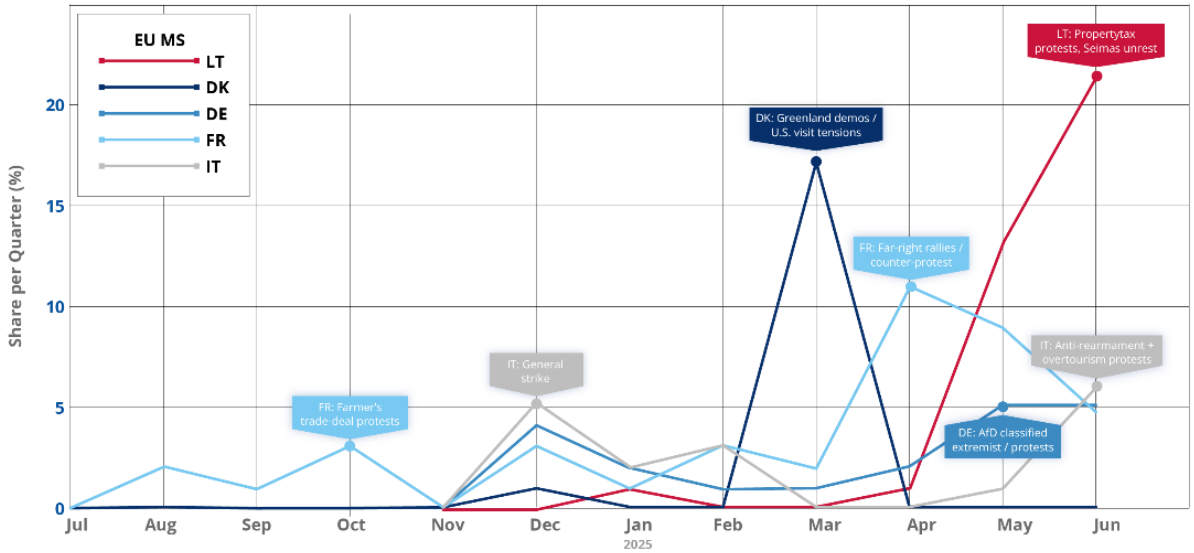
Within the finance sector, incidents are primarily concentrated in the banking subsector, which accounts for 21.6% of cases. The insurance subsector follows at around 3.4%, while blockchain-related services represent an exceedingly small share at less than 1%.

Fig. 23 - Distribution of incidents targeting the EU Finance sector.
Source: ENISA dataset



Banks are also the most targeted subsector by hacktivist groups (69%), likely in an attempt to create nuisances for the users of online banking services, ultimately contributing to the information operation component of hacktivism. NoName057(16) (71.1%), Keymous+ (13.7%) and DarkStorm Team (15.2%) were recorded as being the most active against the finance sector overall. Peaks of activity were notably observed around electoral processes in EU MSs [129], as well as during tense political and societal contexts at the national level in EU MSs, especially when related to polarising topics.

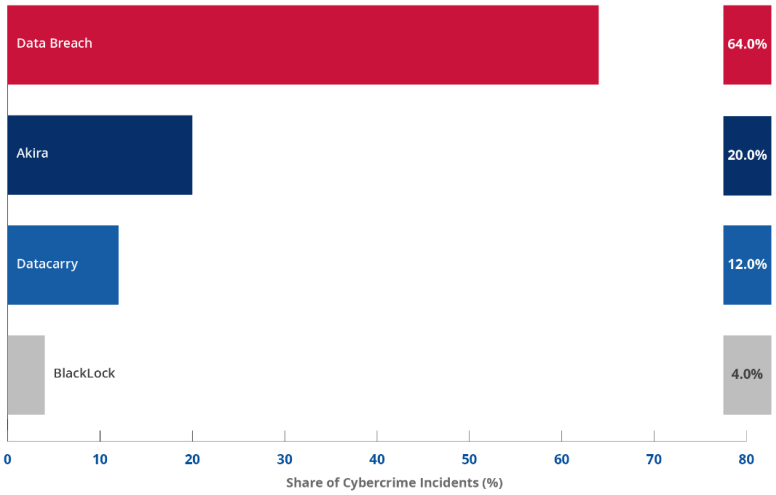
Fig. 24 - Contextualised DDoS against the EU Finance sector.
Source: ENISA



[128] https://ciras.enisa.europa.eu/ciras-consolidated-reporting
[129] hxxps://t.me/Darkstormbackup2/63

As they clearly process a significant amount of financial and personal data, financial institutions represent high value targets for cybercriminals. Data breaches pertaining to the finance sector amounted to 64% while ransomware accounted for 36%. The ransomware strains reportedly deployed against EU financial institutions were Akira (20%), Datacarry (12%) and BlackLock (4%).

Fig. 25 - Cybercrime claims against the EU Finance sector
Source: ENISA dataset



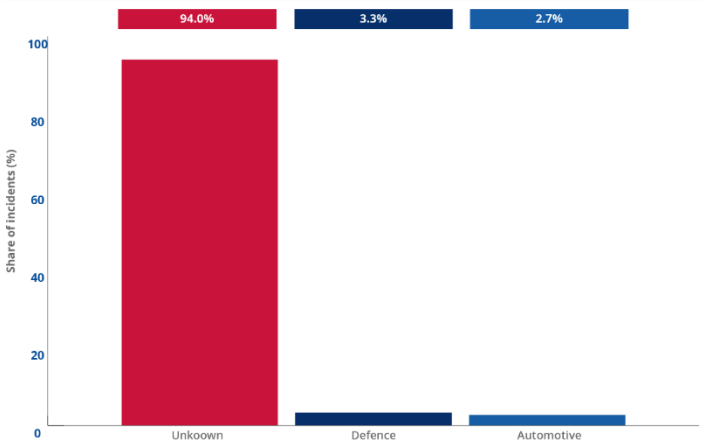
Typically associated with DPRK-nexus intrusion sets, targeting of the finance sector over the reporting period by China-nexus intrusion sets was also observed, with an overall total of two incidents. While the widely-spread nature and lack of granularity of events associated to Lazarus does not allow for a more detailed analysis pertaining to EU organisations [130] and based on Lazarus' previously reported activities, it is highly likely this intrusion set still represents a primary threat to EU financial organisations.

5.5 MANUFACTURING

Despite a rather low share overall (2.9%), the manufacturing sector went from seventh to fourth place among NIS2 sectors compared to ETL 2024.

While a majority of impacted manufacturing organisations were unidentified (94%), the breakdown of identified subsectors shows a clear **focus on defence and automotive related entities.** As websites of these two subsectors were particularly targeted by hacktivist-led DDoS attacks (45.8% of manufacturing targeting by hacktivist groups), it is highly likely this justifies the EU MS ranking, where these EU MSs are perceived as particularly mature in both their defence and automotive sectors.

Fig. 26 - Distribution of incidents against the EU Manufacturing sector.
Source: ENISA dataset



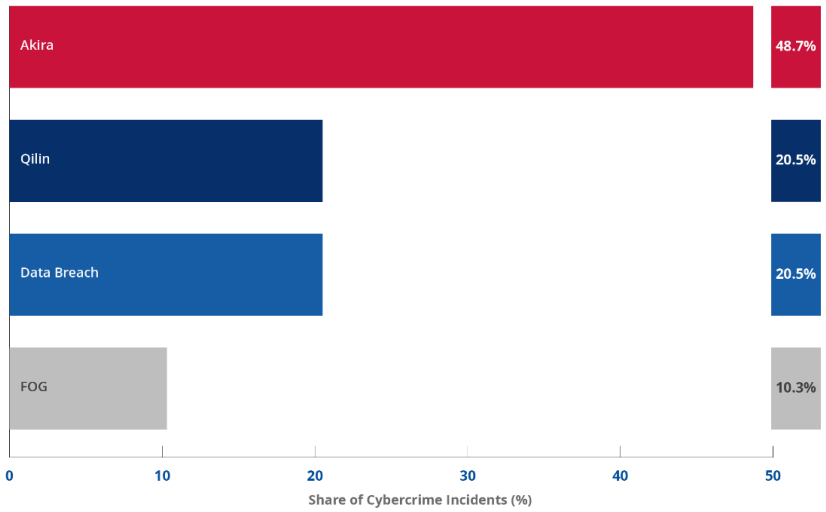
Similarly to the targeting of previously documented sectors, **hacktivist activities against this sector (39.3%) were primarily grounded in the context of the support of Ukraine by EU MSs** and led by NoName057(16) (75.6%). Hacktivist activity targeting the manufacturing sector included DDoS attacks and, in some cases,

[130] https://www.securonix.com/blog/research-update-threat-actors-behind-the-devpopper-campaign-have-retooled-and-are-continuing-to-target-software-developers-via-social-engineering/

attempts to disrupt operational technology systems[131] These campaigns often aimed to publicly associate manufacturers with geopolitical conflicts, particularly when firms were linked to defence supply chains[132] [133].

Cybercrime is reportedly the primary threat to the manufacturing sector, both in terms of level of activity (59.3%) and reported impact. While data breaches accounted for 20.5%, the most deployed ransomware strains include Akira (48.7%), Qilin (20.5%), and FOG (10.3%). In H2 2024, multiple ransomware incidents resulted in prolonged disruptions to the business continuity of EU manufacturing organisations, including an attack by BlackBasta on the German consumer-electronics maker Medion AG that resulted in prolonged IT and website disruptions in November 2024[134] [135], and the targeting of the German Arntz Optibelt Group in August 2024 that impacted their IT systems[136] [137]. These incidents illustrate the impact of ransomware on the manufacturing sector. As both companies operate globally, including in the EU, it is highly likely these attacks also had an impact in other EU MSs.

Fig. 27 - Cybercrime claims against EU Manufacturing sector.
Source: ENISA dataset



Based on reports mentioning the **targeting of the manufacturing sector by State-nexus intrusion sets in the EU**, two incidents were identified, including activity imputed to UNC5221 observed in Germany, while an unidentified China-nexus intrusion set was linked to a broader campaign involving clusters such as PurpleHaze and ShadowPad. This campaign, running from July 2024 to March 2025, affected over 70 global targets, including multiple entities in manufacturing. **It is plausible that part of these activities would pertain to the theft of intellectual property.**

[131] https://cyble.com/blog/hacktivists-attacks-on-critical-infrastructure/
[132] https://www.vikingcloud.com/blog/geopolitics-and-cyber-activism-the-growing-impact-of-hacktivism
[133] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[134] https://www.heise.de/news/Medion-Webseite-und-mehr-derzeit-nicht-erreichbar-10185844.html
[135] https://www.heise.de/news/Medion-Hack-BlackBasta-Ransomware-hat-angeblich-1-5-TB-an-Daten-kopiert-10215926.html
[136] https://www.wiwo.de/unternehmen/industrie/cyber-kriminalitaet-hacker-attackieren-mittelstaendler-optibelt-/29967726.html
[137] https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q3-2024/

6. CYBERCRIME

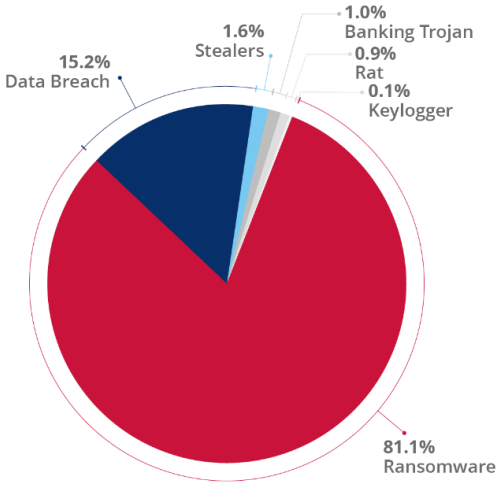
While accounting for 13.4% of all incidents, cybercrime continued to remain a prevalent threat for the short-to-medium term, with encrypting ransomware constituting the most directly impactful threat. Over the reporting period, cybercrime activities targeting EU organisations notably included ransomware (81.1%) and data breaches (15.2%); the latter were specifically documented as resulting from ransomware incidents. The cybercriminal ecosystem structure was regularly impacted by the operations of Law Enforcement Agencies (LEA) and internal competition among cybercriminal groups.

6.1 KEY CYBERCRIME THREATS

Based on monitored Data Leak Sites (DLS) and cybercriminal forums, cybercrime claims accounted for **81% of activities**.

Known EU victims include a broad range of sectors, with at least 36 sectors identified in total, including critical sectors as shown in the NIS2 Directive, with DIS and the manufacturing sector remaining the most impacted in the EU.

Fig. 28 - Distribution of cybercrime claims against EU organisations.
Source: ENISA dataset



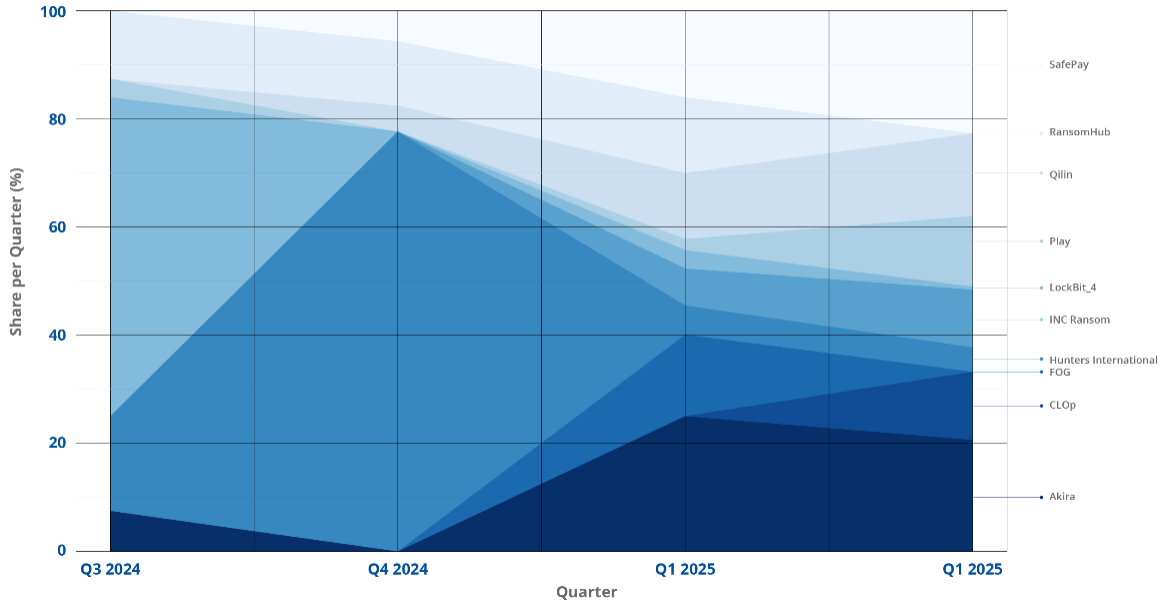
Over the reporting period, data breaches primarily impacted EU digital infrastructure and services (27.7%), notably through the sale of customer data from telecommunications providers, followed by the sale of data related to public administration (17%). Ransomware claims were made primarily against the manufacturing sector (14.9%).

While the recorded share of ransomware deployments remained stable, a **shift in the ransomware ecosystem** was observed over the reporting period, marked by a continuous fragmentation, ultimately leading to the emergence of new ransomware variants and Ransomware-as-a-Service (RaaS) programmes. A total of 82 ransomware variants were reportedly deployed against EU MSs organisations, with Akira emerging as the most frequently deployed (11.6%), followed by SafePay (10.1%), and Qilin (7.5%).

While a few major groups and ransomware strains were particularly prevalent in the previous reporting period, activity in 2024–2025 was more evenly distributed. This evolution is clearly illustrated by LockBit3, which accounted for nearly a quarter of all reported claims over the previous reporting period (ETL 2024) with 198 claims. In May 2025, the LockBit ransomware programme was reportedly compromised resulting in the leak of their internal database, which is likely justifying the absence of claims of this group since 27 May 2025[138] and the emergence of LockBit4 since April, notably leveraged by an operator called Syrphid[139]. Similarly, a decrease in 8Base's deployments followed partial infrastructure leaks and administrator arrests in early 2025[140]. Showing a significant decrease in EU deployments (0.73%) against Austrian, French, German and Italian organisations, BlackBasta stopped claiming incidents altogether since January 2025. In February, the BlackBasta group saw their internal chat messages leaked, exposing disagreements among members as well as its toolset, eventually leading to the group's infrastructure going offline[141] [142].

[138] https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-hacked-victim-negotiations-exposed/
[139] https://www.broadcom.com/support/security-center/protection-bulletin/lockbit-4-0-ransomware
[140] https://www.europol.europa.eu/media-press/newsroom/news/key-figures-behind-phobos-and-8base-ransomware-arrested-in-international-cybercrime-crackdown
[141] https://www.infosecurity-magazine.com/news/blackbasta-ransomwares-ties-russia/
[142] https://www.theregister.com/2025/02/21/experts_race_to_extract_intel/

Fig. 29 - Top 10 ransomware claims in the EU.
Source: ENISA dataset



Akira maintained a continuous but low tempo, SafePay rose to prominence in Q2 2025[143], while Hunters International, which had sustained steady activity in 2024, recorded a decline following a public announcement that it was shutting down in 2025 [144]. RansomHub, previously one of the most deployed ransomware strains in the EU, went offline on 1 April 2025 [145], shortly after increased activity around the formation of a new ransomware alliance led by the DragonForce group.

Info-stealers sold on cybercriminal marketplaces remained a consistent threat vector during the reporting period, primarily facilitating credential theft, session hijacking and access brokering. Although the impact of infostealers' leveraging cannot be assessed, they continue to be key enablers of malware deployments, making them a **solid and prevalent link in the cybercriminal supply chain**, as notably illustrated through the BlackBasta leaks [146].

The info-stealers market observed a significant disruption following **Operation Magnus in October 2024**, which notably led to the dismantling and seizure of the infrastructure of RedLine and META, two prevalent long-running info-stealer families[147] [148]. This led to the **increased use of Lumma info-stealer** by more than 350% between the first and second halves of 2024 [149]. Within the EU, between September 2024 and March 2025 waves of Lumma infections were seen in Italy[150] [151].

[143] https://www.huntress.com/blog/its-not-safe-to-pay-safepay
[144] https://www.bleepingcomputer.com/news/security/hunters-international-rebrands-as-world-leaks-in-shift-to-data-extortion/
[145] https://thehackernews.com/2025/04/ransomhub-went-dark-april-1-affiliates.html
[146] https://www.theregister.com/2025/02/21/experts_race_to_extract_intel/
[147] https://www.eurojust.europa.eu/news/malware-targeting-millions-people-taken-down-international-coalition
[148] https://flashpoint.io/blog/redline-meta-takedown-infostealer/?CRO3=%233007_variant
[149] https://www.eset.com/blog/en/business-topics/threat-landscape/lumma-stealer-threat/
[150] https://cert-agid.gov.it/news/lumma-stealer-diffuso-tramite-notifica-di-falsa-vulnerabilita-di-sicurezza-sul-proprio-progetto-github/
[151] https://cert-agid.gov.it/news/lumma-stealer-e-clickfix-accoppiata-malevola-di-nuovo-in-azione-abusando-di-un-dominio-it/

Lumma Stealer (aka LummaC2 Stealer) is a C language information stealer available through a Malware-as-a-Service (MaaS) model on Russian-speaking forums since at least August 2022[152] [153]. Data is exfiltrated to a C2 server via HTTP POST requests using the user agent TeslaBrowser/5. The stealer also features a non-resident loader that is capable of delivering additional payloads via EXE, DLL, and PowerShell[154], allowing for the leveraging of this malware by ransomware operators and state-nexus intrusion sets[155].

Assessed as having remained the most prevalent info-stealer since the beginning of 2025, Lumma was reportedly deployed on 394,000 Windows machines globally between March and May 2025, with a strong prevalence in the EU [156]. In May 2025, joint international LEA action coordinated by Europol led to the seizing, takedown, suspension and blocking of approximately 2 300 malicious domains in Lumma's infrastructure [157]. A few days following the takedown, Lumma seemingly resumed their operations [158].

Data breaches continued being observed, with high visibility cases pertaining in particular to public administration, digital infrastructure and services, and finance in the EU, and typically sold on forums by Initial Access Brokers (IAB), ultimately leading to their exploitation in follow-up malicious cyber activities, including phishing campaigns. Notable examples during the reporting period included the compromise of contact details for over 62 000 Dutch police staff[159] [160]and the data of 3.2 million Belgian WhatsApp users advertised on BreachForums[161] as well as the personal and banking details of 15 000 customers of Direct Assurance, a French company[162] and claims of stolen source code and credentials of the Swedish company Nokia via a third-party vendor[163].

The IAB economic model was seen to be evolving, notably shifting toward lower-cost, higher-volume sales, with most accesses reportedly priced under EUR 2 800 (about USD 3 000) [164] [165] ; IAB activities also expanded, with a sharp increase of VPN access sale in 2024, while the sale of Personally Identifiable Information (PII) and Remote Desktop Protocol accesses remained stable.

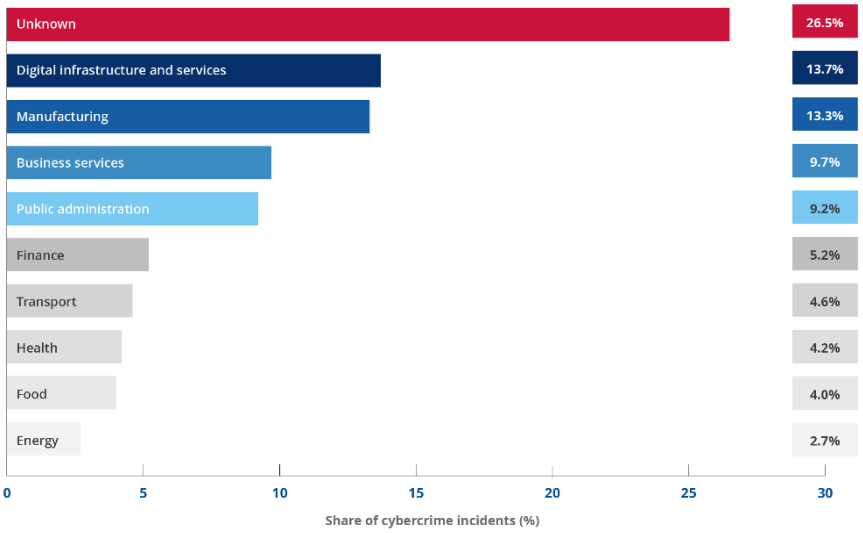
Predictably, **online scamming and fraudulent activity continued**, and was noted over the reporting period. While this type of basic activity is often given less attention in cyber security focused reporting, its simplicity and ubiquity merits at least a cursory mention. Recent cases illustrate how these seemingly 'low-level' scams can evolve into complex, transnational criminal enterprises. In Poland, authorities dismantled an international cybercrime group that impersonated bank and law enforcement officials, defrauding dozens of victims of nearly €570,000 (USD665,000) through spoofed calls and fraudulent transfers [166]. On a much larger scale, a Chinese group named Vigorish Viper was found to be behind illegal online gambling operations advertised across European football stadiums [167]. Vigorish Viper was also linked to human trafficking and cyber fraud compounds in Southeast Asia. Meanwhile, a Dutch court recently sentenced an individual for phishing, bank helpdesk fraud and VIN fraud [168].

[152] https://www.cyfirma.com/research/lumma-stealer-tactics-impact-and-defense-strategies/
[153] https://medium.com/@raghavtiresearch/lumma-stealer-a-proliferating-threat-in-the-cybercrime-landscape-b5cdc3de44a4
[154] https://malpedia.caad.fkie.fraunhofer.de/details/win.lumma
[155] https://www.silentpush.com/blog/lumma-stealer/
[156] https://blogs.microsoft.com/on-the-issues/2025/05/21/microsoft-leads-global-action-against-favored-cybercrime-tool/
[157] https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world%E2%80%99s-largest-infostealer-lumma
[158] https://blog.checkpoint.com/security/lumma-infostealer-down-but-not-out/
[159] https://www.dutchnews.nl/2024/09/police-leak-leaves-data-of-62000-officers-in-hands-of-hackers/
[160] https://www.politie.nl/nieuws/2024/september/27/data.html
[161] https://www.security.nl/posting/854621/Data+3%2C2+miljoen+Belgische+WhatsApp-gebruikers+aangeboden+op+internet?channel=rss
[162] https://www.usine-digitale.fr/article/direct-assurance-victime-d-une-cyberattaque-les-donnees-de-15-000-clients-derobees.N2222978
[163] https://www.bleepingcomputer.com/news/security/nokia-investigates-breach-after-hacker-claims-to-steal-source-code/
[164] https://e.cyberint.com/hubfs/IAB%20Report%202025.pdf
[165] https://socradar.io/the-rise-of-initial-access-brokers-on-the-dark-web/
[166] https://therecord.media/poland-cybercrime-gang-dismantle-impersonation
[167] https://insights.infoblox.com/resources-report/infoblox-report-vigorish-viper-a-venomous-bet
[168] https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBZWB:2025:2524&showbutton=true&keyword=ECLI%253aNL%253aRBZWB%253a2025%253a2524&idx=1

6.2 CYBERCRIME SECTORIAL IMPACT

Cybercriminal activities **continued to impact multiple sectors in the EU in both NIS2 and non-NIS2 sectors**. Over the reporting period, digital infrastructure and services was identified as the most targeted sector (13.7%), followed by manufacturing (13.26%) and business services (9.7%).

Fig. 30 - Cybercrime claims against EU sectors.
Source: ENISA dataset



Within cybercrime activities, ransomware operators primarily claimed attacks against the manufacturing sector (14.9%) and DIS (10.3%). Data breaches were primarily claimed against DIS (28.2%) and public administration (16.8%).

Overall, cybercrime incidents showed a broadly distributed targeting pattern, likely underscoring prioritisation of achieving their lucrative-driven objectives over sector-specific targeting.

In the second half of 2024, multiple ransomware incidents reportedly resulted in service disruption and/or interruption of EU organisations[169] [170] [171] [172] [173] [174] [175] [176]. Of interest is the wave of incidents that impacted the French media industry, with three incidents impacting the sector in less than two months[177] [178] [179]. As leveraged ransomware strains or initial intrusion vectors are not known, it is not possible to assess whether these incidents stemmed from similar entry points, third party attacks or connections to specific geopolitical contexts.

While ransomware attacks inherently impact the confidentiality, integrity and accessibility of data, assessing their economic, operational and reputational impacts remains challenging. Over the reporting period, a limited number of attacks impacting EU companies claimed by ransomware operators were acknowledged, and the operational impact was documented in very few cases. While it is likely some claims are preposterous and ransomware attacks do not systematically impact operations, under-reporting and the superficial documentation of ransomware attacks in open sources are additional reasons for this intelligence gap.

[169] https://therecord.media/kawasaki-europe-cyberattack-operations-restored
[170] https://libertia.es/noticias-en-ciberataques-resumen-2024/
[171] https://www.lemondeinformatique.fr/actualites/lire-ransomware-les-boutiques-de-musees-francais-touchees-94449.html
[172] https://www.cybersecitalia.it/attacco-ransomware-al-comune-di-fabriano-mette-fuori-uso-i-pc-e-causa-disservizi-agli-utenti/37222/
[173] https://www.lemondeinformatique.fr/actualites/lire-ransomware-les-boutiques-de-musees-francais-touchees-94449.html
[174] https://www.bleepingcomputer.com/news/security/lynx-ransomware-behind-electrica-energy-supplier-cyberattack/
[175] https://www.universite-paris-saclay.fr/piratage
[176] https://soziales.provinz.bz.it/de/news/technische-probleme-in-mehreren-zentralen
[177] https://www.lemonde.fr/actualite-medias/article/2024/09/10/le-journal-la-croix-et-le-groupe-bayard-victimes-d-une-cyberattaque-par-rancongiciel_6311493_3236.html
[178] https://www.lemonde.fr/pixels/article/2024/10/25/le-journal-liberation-victime-d-une-attaque-de-type-rancongiciel_6359555_4408996.html
[179] https://www.afp.com/fr/lagence/notre-actualite/communiques-de-presse/attaque-sur-le-systeme-dinformation-de-lafp

While incidents impacting the health sector accounted for only 4.2% of the overall cybercrime incidents identified, ransomware attacks against two German organisations that resulted in the postponement of medical procedures remain of particular concern[180] [181].

Fig. 31 - Example of ransomware incidents leading to operational impact.
Source: ENISA dataset

Sector	Date	Organisation	Impacted EU MS	Reported impact
Transport	07-2024	Split St. Jerome Airport	HR	Flights cancelled/ delayed; manual check-in implemented
Public administration	07-2024	Comune di Fabriano	IT	Digital municipal services disrupted
Media & Entertainment	08-2024	RMN-Grand Palais	FR	Boutiques & webshop disrupted; venues OK
Education	08-2024	Université Paris-Saclay	FR	All internal servers down; weeks in degraded mode
Health	09-2024	Weitzckliniken (Bavaria)	DE	IT outage; operations cancelled; analog fallback
Manufacturing	09-2024	Kawasaki Motors Europe (KME)	NL	Servers isolated after ransomware;EU dealer/supplier ops disrupted
Media & Entertainment	09-2024	Bayard / La Croix	FR	No print edition; tools & e-commerce degraded
Media & Entertainment	09-2024	Agence France-Presse (AFP)	FR	News delivery to clients disrupted
Health	10-2024	Johannestift Diakonie	DE	Central servers encrypted; planned procedures postponed
Media & Entertainment	10-2024	Libération	FR	Print layout blocked; degraded weekend print
Ratail & Commerce	11-2024	Inforsista	ES	Operations paralysed during Black Friday; gradual recovery
Manufacturing	11-2024	U.S. Blue Yonder - > BIC	FR	EU shipping delays at BIC from upstream outage
Energy	12-2024	Electrica Group	RO	Customer-facing IT affected; critical systems isolated
Transport	04-2025	Plus Service / Telemaco	IT	Public transport ticketing systems down for two days; disruption for userd

6.3 CYBERCRIME GEOGRAPHICAL IMPACT

Ransomware incidents continued affecting EU Member States, with a notable shift in geographical impact compared to ETL 2024.

The top five EU MSs referenced in ransomware and data breaches claims include Germany (23.4%), Italy (11.33%), Spain (9.8%), France (9.5%), and Belgium (3.7%). While this ranking could stem from multiple factors, and as analysed by the CCB, it is likely these EU MSs would be seen as major economic players within the EU and thus represent high value targets [182].

During the report period, manufacturing remained the most consistently targeted sector across all five EU MSs. Germany recorded the highest number of claims by SafePay, INC Ransom and Akira, with the most targeted sectors being manufacturing and digital services providers. Italy saw increased activity from Akira, Sarcoma, and Qilin, targeting the manufacturing sector, followed by digital infrastructure and services. Spain saw Qilin in first place, followed by Akira and FOG, with manufacturing being targeted the most, followed by business services and public administration. France was mostly impacted by Qilin, Hunters International, and CL0P, Belgium saw activity from RansomHouse and Play, alongside SafePay and Qilin. In both Belgium and France, manufacturing was the most targeted sector, followed by DIS.

[180] https://www.johannesstift-diakonie.de/presse-aktuelles/aktuelle-meldungen/meldung/670-cyberangriff-auf-die-johannesstift-diakonie
[181] https://www.heise.de/news/Cyberangriffe-betreffen-Wertachkliniken-in-Bayern-und-Londoner-Verkehrsbetrieb-9857069.html
[182] https://ccb.belgium.be/recent-news-tips-and-warning/richer-country-more-ransomware-victims-it-has?

6.4 KEY CYBERCRIME TRENDS

6.4.1 Tactics, Techniques and Procedures (TTPs)

Over the reporting period, cybercriminal groups were seen updating their TTPs, notably through the development or maintenance of their toolsets, as well as their pressure tactics.

Reuse of leaked builders continued to be observed, as illustrated by the SafePay ransomware, suspected of being derived from a modified LockBit3 builder [183]. 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 [184].

While **infostealers** continued to be delivered through cracked software, phishing pages and public code repositories, **new delivery mechanisms** were observed, such as fake CAPTCHA verification pages, cloud-based file hosting services and embedded links in video platforms as well as other high-traffic low-cost delivery vectors[185] [186].

During this reporting period, cybercrime groups started using **tools designed to disable Endpoint Detection and Response (EDR) solutions**, enabling them to conduct stealthier intrusions focused on rapid data exfiltration. In July 2024, FIN7 was observed advertising AvNeutralizer (aka AuKill), a specialised tool for tampering with endpoint defences, to multiple ransomware groups [187]. The tool had been previously linked to intrusions deploying AvosLocker, MedusaLocker, BlackCat/ALPHV, Trigona and LockBit[188], all of which were reportedly active in the EU. In August 2024, RansomHub started using similar tools, as can be seen by their adoption of EDRKillShifter and TDSSKiller —leveraging them to disable EDR protections[189] [190]. In June 2025, variants of EDRKillShifter started to be incorporated in multiple RaaS toolsets, including LockBit, Medusa, and BlackCat/ALPHV[191] [192] [193]. Another technique illustrating this trend is the use of a HeartCrypt-packed loader with the malicious driver ABYSSWORKER in a Medusa ransomware chain, revealing how attackers exploit or bring their own signed drivers to disable EDR systems [194]. Of particular concern in this regard is the reported abuse of a legitimate tool called HRSworld [195], likely to be increasingly observed in cybercriminal activities.

Fog and Qilin, both relatively recent ransomware strains, relied on **aggressive pressure tactics**, including countdown timers, victim profiles and downloadable sample files in double extorsion, targeting reputational damage or regulatory exposure [196], or in the case of Qilin a new 'call lawyer' feature, which mimics legal escalation, pressuring victims to act quickly under the illusion of formal consequences [197]. The legal pressure developments are of particular relevance in the EU, where cyber incident reporting and GDPR obligations are likely to represent an additional incentive for impacted companies to pay the requested ransom.

Additional TTPs of interest over the reporting period include **resorting to physical components** [198]. Observed since at least the mid-2010s in China and globally since 2019 [199], pig-butchering scams [200] are increasingly reported as being leveraged to target citizens in EU MSs. In 2024, pig-butchering scams grew by

[183] https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/safepay-ransomware/
[184] https://x.com/Manu_De_Lucia/status/1924792567461294492
[185] https://blog.checkpoint.com/security/lumma-infostealer-down-but-not-out/
[186] https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-402024#75878-1
[187] https://thehackernews.com/2024/07/fin7-group-advertises-security.html
[188] https://www.sentinelone.com/labs/fin7-reboot-cybercrime-gang-enhances-ops-with-new-edr-bypasses-and-automated-attacks/
[189] https://www.trendmicro.com/en_us/research/24/i/how-ransomhub-ransomware-uses-edrkillshifter-to-disable-edr-and-.html
[190] https://www.threatdown.com/blog/new-ransomhub-attack-uses-tdskiller-and-lazagne-disables-edr/
[191] https://news.sophos.com/en-us/2025/08/06/shared-secret-edr-killer-in-the-kill-chain/
[192] https://www.halcyon.ai/blog/edr-killers-increasingly-used-to-bypass-security-in-ransomware-operations
[193] https://www.eset.com/blog/en/business-topics/threat-landscape/stop-edr-killers/
[194] https://www.elastic.co/security-labs/abyssworker
[195] https://www.theregister.com/2025/03/31/ransomware_crews_edr_killers/
[196] https://stonefly.com/blog/fog-ransomware-malware-targeting-windows-linux/
[197] https://thehackernews.com/2025/06/qilin-ransomware-adds-call-lawyer.html
[198] https://safeonweb.be/nl/actueel/pas-op-voor-nep-cyberbeveiligingsaudits-die-aan-je-bedrijf-worden-aangeboden
[199] https://www.scmp.com/news/people-culture/social-welfare/article/3150688/online-pig-butchering-love-scams-have-gone
[200] Scams in which threat actors spend weeks or months building trust with victims, often through fake online relationships, before defrauding them of their money, often by convincing them to invest in fraudulent cryptocurrency platforms.

almost 40% year-on-year, reportedly generating between €9.1 (USD 10.6) billion and €11.4 (USD 13.3) billion, and accounting for over one-third of global cryptocurrency scam revenue [201]. Throughout this period, open sources noted the increased use of generative AI and deepfake videos to impersonate trusted contacts, enhancing the social-engineering phase of these scams. 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 [202] [203]. Between 10 and 17 September 2024, Europol coordinated an international operation dismantling a mobile-phone phishing network that unlocked over 1.2 million stolen devices; elements of the compromised devices and stolen credentials had been repurposed for pig-butchering outreach and cryptocurrency theft[204].

Of rising and significant concern is the physical targeting, including kidnapping, of crypto-asset holders and their families[205] [206]. These events have been linked to data leaks from centralised crypto exchanges, which often contain PII, including, in some cases, home addresses[207]. Such physical attacks were publicly reported in multiple EU MSs, with several high-profile cases notably in Belgium[208], France[209] and Spain[210].

6.4.2 Evolution of the ecosystem

As previously mentioned, the cybercriminal ecosystem underwent frequent disruptions, stemming from internal competition, alliances and LEA operations[211].

The first half of 2025 notably saw several RaaS shutdowns, including BlackBasta in February[212] [213]and RansomHub in April 2025[214]. The latter was announced to have joined the DragonForce-led coalition alongside RansomBay in the same month[215]. Since then, while DragonForce primarily claimed ransomware incidents in the US, 19 EU MSs organisations were listed on their DLS.

Having faced a coordinated LEA operation as well as sanctions against one of their affiliates also linked to Evil Corp in October 2024[216] [217], LockBit operations were impacted by the compromise, defacement and leaking of their affiliate management panel, and since May 2025 the group seems to have cease their activities. Whether the newly documented LockBit4 operator Syrphid is a former LockBit affiliate was not known at the time of reporting[218].

Multiple operations aiming at disrupting cybercriminal activities across the full supply chain included operations against the communication means of cybercriminals, as illustrated by the dismantling of the Ghost encrypted communications platform in September 2024[219] [220], **cybercrime forums** such as Cracked,

[201] https://www.chainalysis.com/blog/2024-pig-butchering-scam-revenue-grows-yoy/
[202] https://about.fb.com/news/2024/11/cracking-down-organized-crime-scam-centers/
[203] https://www.wired.com/story/pig-butchering-scam-invasion/
[204] 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
[205] https://cointelegraph.com/news/violent-crypto-robberies-rise-six-attacks-investors
[206] https://cointelegraph.com/news/bitcoin-wrench-attacks-to-double-2021-peak
[207] https://cointelegraph.com/news/1-bitcoiner-kidnapped-every-week-cyrpto-exec
[208] https://www.bruxellestoday.be/faits-divers/course-poursuite-enlevement-epouse-cryptomonnaies.html
[209] https://www.theguardian.com/world/2025/may/04/french-police-investigate-spate-of-cryptocurrency-millionaire-kidnappings
[210] https://metro.co.uk/2025/02/09/three-british-men-spain-arrested-kidnap-cryptocurrency-broker-22523644/
[211] https://www.letelegramme.fr/france/un-travail-de-fourmi-comment-des-gendarmes-bretons-ont-traque-un-escroc-qui-exige-des-rancons-6808584.php
[212] https://www.infosecurity magazine.com/news/blackbasta ransomwares ties russia/
[213] https://www.theregister.com/2025/02/21/experts_race_to_extract_intel/
[214] https://thehackernews.com/2025/04/ransomhub-went-dark-april-1-affiliates.html
[215] https://www.infosecurity-magazine.com/news/dragonforce-turf-war-ransomware/
[216] https://www.europol.europa.eu/media-press/newsroom/news/lockbit-power-cut-four-new-arrests-and-financial-sanctions-against-affiliates
[217] https://www.gov.uk/government/news/uk-sanctions-members-of-notorious-evil-corp-cyber-crime-gang-after-lammy-calls-out-putins-mafia-state
[218] https://www.broadcom.com/support/security-center/protection-bulletin/lockbit-4-0-ransomware
[219] https://www.europol.europa.eu/media-press/newsroom/news/global-coalition-takes-down-new-criminal-communication-platform
[220] https://therecord.media/ghost-encrypted-criminal-communications-takedown-arrests

Nulled and BreachForums[221] [222] [223], and the seizure of the **servers of cryptocurrency exchanges** suspected of being used to launder financial flows, notably originating from ransomware operations[224].

The 28 October 2024 takedown of RedLine and META infostealers under Operation Magnus resulted in multiple arrests and server seizures across Europe and the US[225] [226]. These efforts continued with the arrest of four leaders of the 8Base group on 10 February, which significantly reduced Phobos ransomware activity[227]. A subsequent phase of Operation Endgame from 19–22 May 2025 neutralised seven malware families — Bumblebee, Lactrodectus, Qakbot, Hijackloader, DanaBot, Trickbot, and Warmcookie—commonly used by Initial Access Brokers (IAB) to breach victim systems and enable the deployment of ransomware[228].

Law enforcement also focused on dismantling the services and networks that facilitate other forms of cybercrime. On 4 June 2024, Portuguese and Spanish authorities arrested 54 suspects in a vishing operation[229]. Between 10–17 September, Europol coordinated an operation with Ameripol that dismantled a phishing network, which unlocked over 1.2 million stolen mobile phones and resulted in 17 arrests[230].

Other notable takedowns included the arrest of a suspect linked to DoppelPaymer ransomware in Moldova on 12 May[231] [232] [233], and Operation Macefall on 21 May, which seized over 2 300 domains tied to LummaStealer infostealer operations[234]. The month also saw authorities take down a group providing crypting and counter-antivirus services on 27 May[235].

[221] https://www.europol.europa.eu/media-press/newsroom/news/international-operation-against-phone-phishing-gang-in-belgium-and-netherlands
[222] https://operation-endgame.com/
[223] https://www.europol.europa.eu/media-press/newsroom/news/operation-endgame-strikes-again-ransomware-kill-chain-broken-its-source
[224] https://www.fiod.nl/seizure-of-7-million-euros-of-crypto-currency-and-2-crypto-currency-exchanges-offline/
[225] https://www.eurojust.europa.eu/news/malware-targeting-millions-people-taken-down-international-coalition
[226] https://www.operationmagnus.com/
[227] https://www.europol.europa.eu/media-press/newsroom/news/key-figures-behind-phobos-and-8base-ransomware-arrested-in-international-cybercrime-crackdown
[228] https://www.bleepingcomputer.com/news/security/moldova-arrests-suspect-linked-to-doppelpaymer-ransomware-attacks/
[229] https://www.europol.europa.eu/media-press/newsroom/news/call-blocked-hard-and-fast-action-against-54-spanish-phone-fraudsters
[230] 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
[231] https://www.justice.gov/usao-ndok/pr/botnet-dismantled-international-operation-russian-and-kazakhstani-administrators
[232] https://blog.lumen.com/black-lotus-labs-helps-demolish-major-criminal-proxy-network/
[233] https://www.bleepingcomputer.com/news/security/moldova-arrests-suspect-linked-to-doppelpaymer-ransomware-attacks/
[234] https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world%E2%80%99s-largest-infostealer-lumma
[235] https://blogs.microsoft.com/on-the-issues/2025/05/21/microsoft-leads-global-action-against-favored-cybercrime-tool/

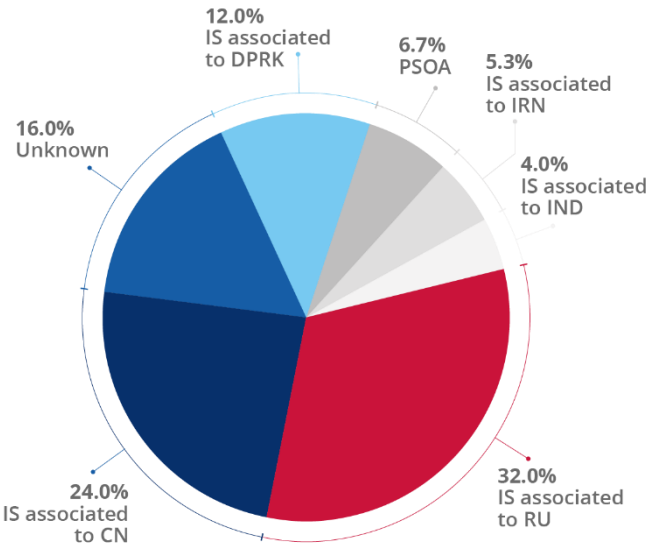
7. STATE-ALIGNED ACTIVITIES

In this section, 'nexus' should be understood as aligned or associated to some extent to a specific country, as reported in open sources, based on public attributions from national, EU and non-EU authorities as well as high confidence imputation by trusted private vendors.

State-aligned adversaries tracked by ENISA include state-nexus intrusion sets, hackers-for-hire, faketivists and private sector offensive actors (PSOAs). While also considered a part of state-aligned activities, Intrusion Manipulation Sets (IMS) involved in information operations are covered in a separate dedicated section of this report.

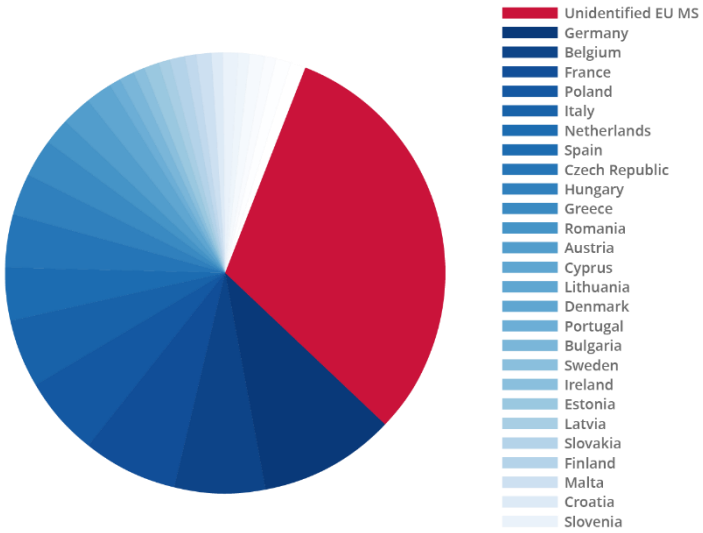
Among state-aligned adversaries, **46 distinct intrusion sets were observed to be active in the EU** over the reporting period. Approximately 14.2% of state-aligned malicious cyber activities were not imputed to a known or newly documented intrusion set, with Russia-nexus recording the highest number of unidentified intrusion sets (47%), followed by China-nexus (43%) and DPRK-nexus (36%). This gap likely stems from shifts in or the emergence of observed Tactics, Techniques and Procedures (TTPs) and toolsets leveraged by Intrusion Sets, known offensive cyber doctrines of specific nexuses (i.e. usage of front companies, contractors, digital quartermasters) and the diverse tracking and reporting practices of private vendors. While this lack of association does not impact detection strategy, it is likely to hinder accurate situational awareness and preparedness efforts.

Fig. 32 - State-aligned offensive cyber activities against EU.
Source: ENISA dataset



Between July 2024 and July 2025, 7.2% of incidents associated with state-aligned activities against EU MSs were identified, with Russia-nexus intrusion sets documented as the most active, followed by China-nexus and DPRK-nexus intrusion sets. Over the reporting period, **outliers were identified, notably with activities carried out by India-nexus intrusion sets**. While accounting for a low share, state-aligned cyberespionage remains a primary concern in the medium-to-long term.

Fig. 33 - State-aligned offensive cyber activities against EU.
Source: ENISA dataset



Almost all EU MSs were reportedly targeted by State-aligned offensive cyber activities. While no information related to the targeting of Luxembourg was identified in open sources, it is plausible the targeting of this MS would be conflated in the 'unidentified EU MS' category. Accounting for 38% of the total number of reported targeting, this category notably includes vague phrasing documented in open-source reports such as 'Western Europe', 'Southern Europe', or 'EU country'.

From a sectorial vantage point, the top five targeted NIS2 sectors in the EU by State-aligned threat groups based on open-source reports include public administration, transport, digital infrastructure, energy and health. As mentioned before, this ranking comes with multiple caveats, based on unspecified or non-granular reporting – notably exemplified by the 'unknown' and 'private companies' categories accounting for 33% of all recorded targeting as well as differences in sectorial worldwide reporting conventions. However, as will be detailed in the following sections and based on historical reporting, this graph is assessed to be a realistic snapshot of sectorial targeting by State-aligned intrusion sets.

7.1 KEY STATE-ALIGNED THREATS

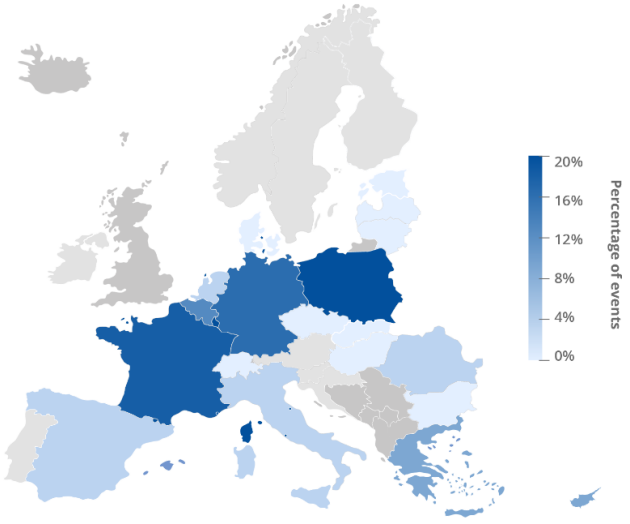
7.1.1 Russia-nexus intrusion sets

Reportedly the most active over the reporting period, Russia-nexus intrusion sets continuously targeted EU MSs in cyberespionage campaigns.

The most documented intrusion sets include APT29, followed by APT28, and Sandworm. Overall, Russia-nexus offensive cyber activities targeted the public administration with a clear focus on governmental and diplomatic entities, the defence sector and the digital infrastructure sector. While targeting multiple EU MSs, geographical targeting in the EU indicates a focus on Poland, France, Germany, Belgium and Greece.

Both **sectorial and geographical targeting are likely to be partly related to EU MSs' support for Ukraine, in the context of Russia's war of aggression against Ukraine since February 2022.**

Fig. 34 - Reported Russia-nexus intrusion sets activities in the EU.
Source: ENISA dataset



This is notably exemplified by spearphishing campaigns for cyberespionage purposes targeting EU MSs, with a particular focus on transport[236] [237], defence and logistics related entities as well as telecommunications infrastructures[238] [239] and embassies carried out by **APT28**. This intrusion set was also observed targeting political parties and institutions[240].

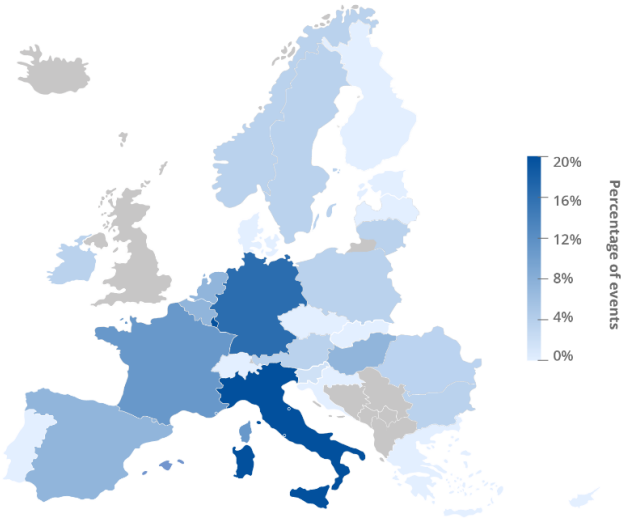
In the aftermath of its successful compromise of Microsoft systems in January 2024[241] [242] , **APT29** was reported to be conducting a global rogue RDP campaign using spearphishing emails to target multiple EU MSs, the European Space Agency (ESA) and NATO Enterprise[243] [244] [245] [246]. Registration of the identified infrastructure reportedly started as early as August 2024, with domains notably impersonating Amazon and Microsoft services and masquerading as organisations in the government, NGO, military and IT sectors. APT29 was also seen resuming their wine tasting event spearphishing campaign, masquerading as an EU MS embassy to target EU Ministries of Foreign Affairs[247].

Finally, assessed to be particularly advanced intrusion sets, **Turla and Sandworm** were both reported active in the EU. While focused on conducting cyberespionage and disruptive campaigns against Ukraine, Sandworm's apparent mandate still pertains to the energy vertical[248] [249], notably illustrated by its targeting of a gas storage entity in an EU MS, as well as a spearphishing campaign targeting attendees at an EU-based natural gas conference[250]. Turla was reported as conducting a long-standing cyberespionage campaign seemingly focused on one specific EU MS, with multiple attempts against governmental entities between January 2024 and May 2025[251].

[236] https://www.br.de/nachrichten/deutschland-welt/cyber-attacke-auf-deutsche-flugsicherung,UN7rsL4
[237] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/250521_Sicherheitshinweis_GRU-Einheit_26165.html,
[238] https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/ce-que-l-on-sait-sur-les-cyberattaques-de-pirates-pro-russes-contre-des-collectivites-francaises_6988775.html
[239] https://media.defense.gov/2024/Feb/27/2003400753/-1/-1/0/CSA-Russian-Actors-Use-Routers-Facilitate-Cyber_Operations.PDF
[240] https://www.bitdefender.com/en-gb/blog/businessinsights/uac-0063-cyber-espionage-operation-expanding-from-central-asia
[241] https://www.ic3.gov/CSA/2024/241010.pdf
[242] https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/
[243] https://www.volexity.com/blog/2025/02/13/multiple-russian-threat-actors-targeting-microsoft-device-code-authentication/
[244] https://www.volexity.com/blog/2025/04/22/phishing-for-codes-russian-threat-actors-target-microsoft-365-oauth-workflows/
[245] https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/
[246] https://www.trendmicro.com/en_us/research/24/l/earth-koshchei.html
[247] https://www.volexity.com/blog/2025/02/13/multiple-russian-threat-actors-targeting-microsoft-device-code-authentication/
[248] https://www.microsoft.com/en-us/security/blog/2025/02/12/the-badpilot-campaign-seashell-blizzard-subgroup-conducts-multiyear-global-access-operation/
[249] https://cert.gov.ua/article/6282517
[250] https://strikeready.com/blog/ru-apt-targeting-energy-infrastructure-unknown-unknowns-part-3/
[251] https://www.welivesecurity.com/en/eset-research/moon-backdoors-lunar-landing-diplomatic-missions/

7.1.2 China-nexus intrusion sets

Fig. 35 - Reported China-nexus intrusion sets activities in the EU.
Source: ENISA dataset



The top five China-nexus intrusion sets active in the EU include UNC5221 (reportedly overlapping with Volt Typhoon), Mustang Panda, APT41, Flax Typhoon and Salt Typhoon. The overall targeting of China-nexus intrusion sets in the EU indicates a focus on the public administration, transport, civil society and digital infrastructure sectors, as well as consistent cyberespionage campaigns against Italy, Germany, France and Belgium.

A more granular analysis of the sectorial targeting by these intrusion sets shows a particular interest in targeting governments and diplomatic entities, aviation and maritime industries, NGOs and human rights advocacy groups and telecommunications. Slowly emerging as outliers is the targeting of food manufacturing and agricultural research. It is likely these campaigns pertain to **strategic data collection and intellectual property theft, mirroring China's Made in China 2025 (MIC 2025) goals for the acquisition of technology and transport connectivity related to China's Belt and Road project and logistics strategies in Europe**. Civil society targeting likely reflects domestic priorities around narrative control and the monitoring of dissident or diaspora networks.

While reportedly increasing in Asia, documented China-nexus cyber threats in the EU was particularly inflated by the compromise of edge devices, notably leveraged in Operational Relay Boxes (ORBs) for follow-up offensive cyber activities, as exemplified by campaigns associated to **UNC5221**[252] [253] [254]reportedly impacting telecommunication providers, manufacturing, aerospace and public administration in the EU.

A similar pattern was seen with **Flax Typhoon's** leveraging of the Quad7 botnet, compromising thousands of TP-link routers in Europe[255] [256] [257] [258] [259]. **Mustang Panda** and **APT41** demonstrated a clear focus on maritime and shipping industries, leveraging updated TTPs and toolsets[260] [261] [262] [263] [264] [265] [266][267] [268] [269]. Mustang Panda was also seen targeting governments and defence-related events in the EU[270].

Finally, and of particular concern, is the targeting of the telecommunications sector by China-nexus intrusion sets, which is reportedly the unique focus of Liminal Panda, Locksmith Panda and Salt Typhoon[271]; these

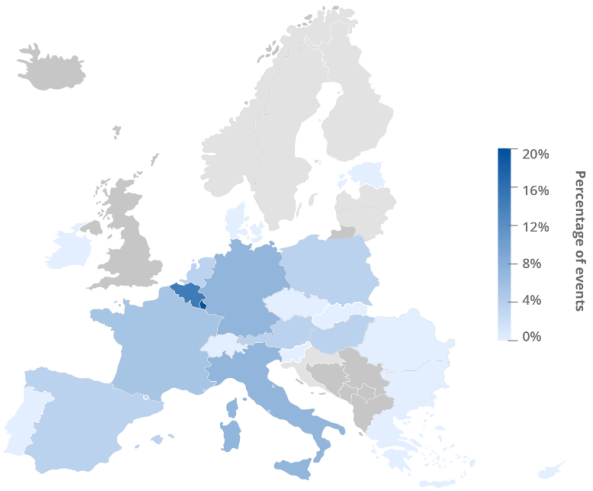
[252] https://news.sophos.com/en-us/2024/10/31/pacific-rim-neutralizing-china-based-threat/
[253] https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day/?hl=en
[254] https://blog.eclecticiq.com/china-nexus-threat-actor-actively-exploiting-ivanti-endpoint-manager-mobile-cve-2025-4428-vulnerability
[255] https://gi7w0rm.medium.com/the-curious-case-of-the-7777-botnet-86e3464c3ffd
[256] https://blog.sekoia.io/solving-the-7777-botnet-enigma-a-cybersecurity-quest/
[257] https://www.team-cymru.com/post/botnet-7777-are-you-betting-on-a-compromised-router
[258] https://media.defense.gov/2024/Sep/18/2003547016/-1/-1/0/CSA-PRC-LINKED-ACTORS-BOTNET.PDF
[259] https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks/
[260] https://blog.talosintelligence.com/chinese-hacking-group-apt41-compromised-taiwanese-government-affiliated-research-institute-with-shadowpad-and-cobaltstrike-2/
[261] https://www.trendmicro.com/en_us/research/24/i/earth-baxia-spear-phishing-and-geoserver-exploit.html
[262] https://www.fortinet.com/blog/threat-research/threat-actors-exploit-geoserver-vulnerability-cve-2024-36401
[263] https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust
[264] https://www.trendmicro.com/en_us/research/24/h/earth-baku-latest-campaign.html
[265] https://www.elastic.co/security-labs/grimresource
[266] https://www.tgsoft.it/news/news_archivio.asp?id=1568
[267] https://www.zscaler.com/blogs/security-research/dodgebox-deep-dive-updated-arsenal-apt41-part-1
[268] https://www.zscaler.com/blogs/security-research/moonwalk-deep-dive-updated-arsenal-apt41-part-2
[269] https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q4-2023-q1-2024.pdf
[270] https://hunt.io/blog/toneshell-backdoor-used-to-target-attendees-of-the-iiss-defence-summit
[271] https://go.crowdstrike.com/2025-global-threat-report.html

were increasingly reported in Asia and the US. In the EU, **Salt Typhoon** has been active since at least December 2024, with activities continuing in 2025, with at least three EU MSs impacted[272] [273].

7.1.3 North Korea-nexus intrusion sets

Over the reporting period, DPRK-nexus intrusion sets were also seen to be active in the EU, particularly in Belgium, Italy, Germany and France. Famous Chollima was reportedly the most active, followed by Lazarus and Kimsuky. **DPRK-nexus activity is heavily skewed toward EU private companies, with a focus on Human Resources, financial services (including crypto) and technology**[274] [275].

Fig. 36 - Reported DPRK-nexus intrusion sets activities in the EU.
Source: ENISA dataset



In addition to continuous job-themed campaigns notably conducted by **Lazarus** to target EU entities involved in the defence, aerospace, media, health and energy sectors[276] [277] [278], **Famous Chollima was seen as increasingly active**, seeking employment as IT workers globally, including in EU companies, notably defence and government-related entities[279] [280] [281] [282] [283] [284].

Following sanctions and indictments from US authorities[285] [286] [287] [288], Famous Chollima reportedly increased their activities in the EU since at least Q4 2024[289] [290] [291] [292] [293] [294]. As an illustration of historical dual motivated DPRK-nexus alleged objectives, Famous Chollima operators were seen carrying out cyberespionage through strategic data collection and were reportedly leveraging extortion schemes upon termination of their contracts to generate revenues[295].

While being continuously active against the Republic of Korea over the reporting period, Kimsuky was observed targeting a RoK based EU defence company and is suspected of having conducted spearphishing activities against EU embassies[296].

[272] https://go.recordedfuture.com/hubfs/reports/cta-cn-2025-0213.pdf
[273] https://blog.talosintelligence.com/salt-typhoon-analysis/
[274] https://securityscorecard.com/blog/operation-99-north-koreas-cyber-assault-on-software-developers/
[275] https://blog.sekoia.io/clickfake-interview-campaign-by-lazarus/
[276] https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q2-2024-q3-2024.pdf
[277] https://cloud.google.com/blog/topics/threat-intelligence/unc2970-backdoor-trojanized-pdf-reader
[278] https://www.microsoft.com/en-us/security/blog/2024/08/30/north-korean-threat-actor-citrine-sleet-exploiting-chromium-zero-day/
[279] https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/EN/2024/2024-10-01-private-sector-security-advisory.html
[280] https://www.knowbe4.com/hubfs/North-Korean-Fake-Employees-Are-Everywhere-WP_EN-us.pdf
[281] https://cloud.google.com/blog/topics/threat-intelligence/mitigating-dprk-it-worker-threat/
[282] https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/2024-10-01-security-advisory.pdf
[283] https://go.crowdstrike.com/2024-threat-hunting-report.html
[284] https://go.crowdstrike.com/2025-global-threat-report.html
[285] https://www.justice.gov/opa/pr/justice-department-disrupts-north-korean-remote-it-worker-fraud-schemes-through-charges-and
[286] https://www.justice.gov/opa/pr/fourteen-north-korean-nationals-indicted-carrying-out-multi-year-fraudulent-information
[287] https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote
[288] https://home.treasury.gov/news/press-releases/jy2790
[289] https://reports.dtexsystems.com/DTEX-Exposing+DPRK+Cyber+Syndicate+and+Hidden+IT+Workforce.pdf
[290] https://go.recordedfuture.com/hubfs/reports/cta-nk-2025-0213.pdf
[291] https://cloud.google.com/blog/topics/threat-intelligence/dprk-it-workers-expanding-scope-scale/
[292] https://6068438.fs1.hubspotusercontent-na1.net/hubfs/6068438/saja-dprk-employment-scam-network.pdf
[293] https://news.sophos.com/en-us/2025/05/08/nickel-tapestry-expands-fraudulent-worker-operations/
[294] https://www.trendmicro.com/en_be/research/25/d/russian-infrastructure-north-korean-cybercrime.html
[295] https://assets.sophos.com/X24WTUEQ/at/wwf5phjtj9bjvmpqqsbfxc/sophos-2024-threat-report.pdf
[296] https://www.spiegel.de/netzwelt/web/diehl-defence-hacker-aus-nordkorea-zielen-auf-mitarbeiter-des-ruestungskonzerns-a-8735f440-670c-40df-9e46-06c620fe9be6

7.1.4 Rest of the World (RoW)

Other state-nexus activities targeting the EU over the reporting period included offensive cyber operations associated to India, Iran and PSOAs. **Shifting from their historical regional targeting and emerging in the EU in Q2 2024, India-nexus intrusion sets** including Bitter and SideWinder conducted continuous spearphishing campaigns, notably against EU embassies throughout the reporting period[297] [298] [299]. Their activities used lures with names referencing EU–India trade negotiations, security dialogues or maritime cooperation, likely reflecting India's interest in understanding EU policy positions in the Indo-Pacific, maritime security frameworks and technology transfer controls.

The activities of Iran-nexus intrusion sets displayed a low tempo with a narrow and clear focus on civil society and NGOs, followed by public administration and transport. Active intrusion sets in the EU over the reporting period include **MuddyWater**[300], **APT42**[301], **Charming Kitten**[302], and subclusters **UNC3313** and **UNC5667**[303]. While the targeting of civil society and NGOs aligns with the historical activities of Iran-nexus intrusion sets for the surveillance of Iran's diaspora and dissidents in the EU, it is likely the targeting of an EU MS government would have been driven by the 12-day war between Israel and Iran.
Reportedly linked to Belarus, **Ghostwriter** continuously targeted Poland in spearphishing campaigns against its public administration, specifically governmental and institutional entities[304] while continuing focusing on Ukrainian targets.

Assessed to likely be a spill over of offensive cyber activities in the context of conflicts, pro-Houthi intrusion sets **OilAlpha**[305] and **Rare Werewolf**[306] were reported impacting EU individuals and organisations on at least one occasion over the reporting period.

Finally, the abuse of technologies commercialised by **Private Sector Offensive Actors**, including Candiru, NSO Group and Paragon Solutions continued targeting civil society in the EU. In July 2024, German MEP Daniel Freund declared having been targeted by an attempt to deploy the **Candiru** spyware on his phone two weeks before elections for the EU Parliament[307]. Between December 2024 and February 2025, **Pegasus** spyware infections were identified, with victims in Czech Republic, Poland and Spain. Victimology reportedly included professionals in real estate, logistics and finance, as well as one European government official[308] [309] [310]. Since the beginning of January 2025, open-source reports documenting the use of **Graphite** spyware through the exploitation of 0-day vulnerabilities in WhatsApp's end-to-end encryption and a zero-click iMessage vulnerability tracked as CVE-2025-43200 emerged, reportedly targeting 90 individuals globally, including in at least 15 EU MSs[311] [312] [313] [314] [315] [316] [317] [318] [319] [320].

[297] https://www.proofpoint.com/us/blog/threat-insight/bitter-end-unraveling-eight-years-espionage-antics-part-one
[298] https://www.threatray.com/blog/the-bitter-end-unraveling-eight-years-of-espionage-antics-part-two
[299] https://securelist.com/sidewinder-apt-updates-its-toolset-and-targets-nuclear-sector/115847/
[300] https://research.checkpoint.com/2024/new-bugsleep-backdoor-deployed-in-recent-muddywater-campaigns/
[301] https://www.politico.eu/article/european-parliament-iran-delegation-chair-victim-tehran-linked-hacking-hannah-neumann/
[302] https://unit42.paloaltonetworks.com/iranian-attackers-impersonate-model-agency/
[303] https://x.com/ClearskySec/status/1922298090528375118
[304] https://cert.pl/en/posts/2025/06/unc1151-campaign-roundcube/
[305] https://go.recordedfuture.com/hubfs/reports/cta-2024-0709.pdf
[306] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen.html
[307] https://x.com/daniel_freund/status/1816380995475472771
[308] https://iverify.io/blog/how-democratizing-threat-hunting-is-changing-mobile-security
[309] https://therecord.media/pegasus-spyware-infections-iverify
[310] https://welcome.iverify.io/hubfs/iVerify-Nickname-Vulnerability-Report.pdf
[311] https://citizenlab.ca/2025/06/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted/
[312] https://euvd.enisa.europa.eu/vulnerability/CVE-2025-43200
[313] https://www.theguardian.com/technology/2025/jan/31/whatsapp-israel-spyware
[314] https://www.dpa.gr/el/enimerwtiko/deltia/ereynes-tis-arhis-gia-efarmogi-tn-kai-gia-kakoboylo-logismiko
[315] https://therecord.media/italy-paragon-spyware-targeted-european-victims-whatsapp
[316] https://www.theguardian.com/technology/2025/feb/03/critic-of-italy-libya-migration-pact-told-he-was-target-of-israeli-spyware
[317] https://www.theguardian.com/technology/2025/feb/06/owner-of-spyware-used-in-alleged-whatsapp-breach-ends-contract-with-italy
[318] https://support.apple.com/en-ca/102174
[319] https://www.governo.it/it/articolo/nota-di-palazzo-chigi/27601
[320] https://documenti.camera.it/_dati/leg19/lavori/documentiparlamentari/IndiceETesti/034/004/INTERO.pdf

7.2 KEY STATE-ALIGNED TRENDS

7.2.1 Tactics, Techniques and Procedures (TTPs)

This section provides an overview of Tactics, Techniques and Procedures leveraged by State-aligned intrusion sets, as well as reported toolset developments. These are thoroughly documented in the appendix.

Most commonly seen TTPs leveraged across state-aligned intrusion sets include:

- **Spearphishing**
- **Exploitation of public-facing services and use of default credentials**
- **Execution via PowerShell**, credential brute-forcing and USB-based attacks

State-aligned intrusion sets continued updating and developing their toolsets to gain foothold and maintain stealth and persistent access to targeted information systems. Related key observations include:

- **Innovative physical-layer-adjacent access vectors: Nearest-Neighbour Wi-Fi and Air-Gap Targeting**: APT28's nearest neighbour Wi-Fi attack[321] enabled network breaches from adjacent infrastructures without direct proximity, while GoldenJackal demonstrated infiltration of air-gapped systems via malicious USB drives.
- **Networking and infrastructure exploitation**: Threat actors compromise core network devices through the exploitation of zero-day and n-day vulnerabilities, such as UNC3886 targeting Juniper routers and Velvet Ant exploiting Cisco NX-OS zero-days.
- **Continuous shifts in programming languages**: Re-implementation of existing toolsets in new languages to evade detection and improve portability. GoldenJackal transitioned from C# to Go, while APT35's Cyclops is a Go-based successor to BellaCiao.
- **Anti-detection and evasion mechanisms**: Multiple toolsets incorporate sandbox detection, obfuscation or legitimate software abuse to avoid security controls. Examples include SnipBot's anti-sandbox checks and Mustang Panda's abuse of Microsoft processes for injection.
- **Expanded targeting of Linux systems**: Linux systems, especially in infrastructure and cloud environments, are targeted by malware such as WolfsBane, FireWood, and POOLRAT.
- **In-Memory malware deployment**: Adversaries increasingly execute payloads entirely in memory, as seen in BackdoorDiplomacy's QSC framework and APT29's GRAPELOADER.

7.2.2 EU as a target, and as a lure

Over the reporting period, multiple state-nexus intrusion sets continued leveraging **tailored lures impersonating EU institutions, officials and affiliated entities**. These campaigns capitalised on the perceived legitimacy of EU branding, official communication styles, and references to policy-related events to increase the likelihood that recipients would engage with malicious content. This is notably illustrated by APT29 impersonating an EU Ministry of Foreign Affairs or referencing fictitious diplomatic events and cultural activities to target diplomatic staff in spearphishing campaigns, as well as mentioning ENISA in lure documents aimed at private companies. Similar examples include Callisto's tailored phishing pages to mimic EU institutional correspondence[322], Storm-2372 masquerading as a member of the European Parliament's Committee on Foreign Affairs[323], Laundry Bear' spearphishing campaign posing as organisers of the European Defence & Security Summit in Brussels[324], and UTA0352 and UTA0355 impersonating officials from EU Member States such as Romania and Bulgaria, and Ukraine's diplomatic missions to the EU and NATO[325]. Additional use of the EU brand was illustrated by Earth Preta, a subgroup of APT41, embedding malware in

[321] https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/EN/2024/2024-10-01-private-sector-security-advisory.html
[322] https://citizenlab.ca/2024/08/sophisticated-phishing-targets-russias-perceived-enemies-around-the-globe/
[323] https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/
[324] https://www.microsoft.com/en-us/security/blog/2025/05/27/new-russia-affiliated-actor-void-blizzard-targets-critical-sectors-for-espionage/
[325] https://www.volexity.com/blog/2025/04/22/phishing-for-codes-russian-threat-actors-target-microsoft-365-oauth-workflows/

foreign policy briefings disguised as legitimate EU institutional documents[326], UNC3313 and UNC5667 impersonating the Hungarian government[327], Charming Kitten posing as EU-based journalists and think-tank researchers[328] and Kimsuky leveraging EU-branded diplomatic meeting invitations containing malicious macros[329].

As previously mentioned, multiple state-nexus intrusion sets **leveraged or compromised EU-based infrastructure to host C2 servers or support follow-up cyberattacks**. Such tactics help obfuscate the true origin of traffic, exploit the trust associated with EU network assets and risk implicating EU countries in malicious activity purely on the basis of IP address attribution. China-linked intrusion sets made especially extensive use of EU infrastructure through Operational Relay Box (ORB) networks, incorporating devices, servers and hosting services in the EU[330]. In other cases, EU-hosted servers were used to deliver second-stage payloads, such as the Remcos backdoor, in campaigns targeting Ukraine[331]. Since 2023, Turla configured its KAZUAR backdoor to communicate via compromised WordPress installations hosted within the EU, further embedding malicious infrastructure in trusted environments[332].

From Q3 2024 to Q2 2025, multiple state-nexus intrusion sets **targeted EU entities outside EU territory**—focusing on diplomatic missions, development programmes, commercial operations and cultural institutions. These operations often aligned with the geopolitical priorities of associated nexuses, prioritising intelligence collection on foreign policy, trade negotiations and multilateral security cooperation. This is exemplified by campaigns carried out by Russia-nexus intrusion sets APT29 targeting EU diplomatic missions abroad[333]. This is of particular concern, as overseas missions and affiliated organisations maintain regular contact with Brussels and EU Member State capitals, so compromises could facilitate lateral movement into core EU networks. This operational reality underscores the advantage adversaries gain by focusing on outposts in third countries, where strategic data can be collected in potentially more permissive environments.

State-nexus intrusion sets also **targeted non-EU diplomatic missions, international organisations and commercial entities operating within EU territory**, as exemplified by Callisto targeting Russian exiles in the EU, Charming Kitten leveraging journalist personas to approach Middle Eastern embassy staff stationed in European capitals[334], Earth Preta targeting Asian diplomatic missions in EU capitals[335], and TAG-100 conducting reconnaissance activities against the Cuban embassy in France[336]. In August 2024, as part of Operation AkaiRyū, MirrorFace was reportedly seen for the first time in the EU. Based on MirrorFace's historical focus on Japan, it is highly likely that targeting the EU served as a vector to target Japanese entities[337].

[326] https://www.cyfirma.com/research/apt-profile-mustang-panda/
[327] https://x.com/ClearskySec/status/1922298090528375118
[328] https://blog.checkpoint.com/security/educated-manticore-reemerges-iranian-spear-phishing-campaign-targeting-high-profile-figures/
[329] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/MTAC-East-Asia-Report.pdf
[330] https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks
[331] https://any.run/malware-trends/remcos
[332] https://www.microsoft.com/en-us/security/blog/2024/12/11/frequent-freeloader-part-ii-russian-actor-secret-blizzard-using-tools-of-other-groups-to-attack-ukraine
[333] https://research.checkpoint.com/2025/apt29-phishing-campaign/
[334] https://blog.checkpoint.com/security/educated-manticore-reemerges-iranian-spear-phishing-campaign-targeting-high-profile-figures/
[335] https://www.cyfirma.com/research/apt-profile-mustang-panda/
[336] https://go.recordedfuture.com/hubfs/reports/cta-2024-0716.pdf
[337] https://www.welivesecurity.com/en/eset-research/operation-akairyu-mirrorface-invites-europe-expo-2025-revives-anel-backdoor/

8. FOREIGN INFORMATION MANIPULATION AND INTERFERENCE

8.1 KEY FIMI THREATS

This section was jointly written by ENISA and EEAS STRATCOM. Over the reporting period, multiple EU MSs were targeted by FIMI, primarily carried out by Russia-aligned Information Manipulation Sets, with increased activities around electoral events.

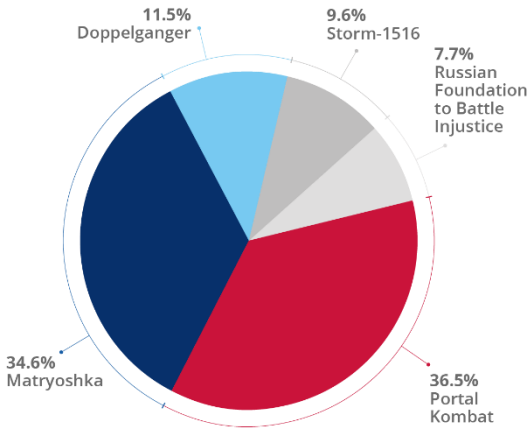
8.1.1 Russia-aligned Information Manipulation Sets

EEAS collected 86 FIMI operations targeting EU entities or EU MSs institutions. Known Information Manipulation Sets (IMS) accounted for 60.5% of all identified cases.

Russia-aligned IMS, including Doppelgänger, Matryoshka, Storm-1516, the Russian Foundation to Battle Injustice and Portal Kombat, conducted FIMI operations against specific EU entities and EU MSs public institutions, notably in France, Germany and Poland. Heavily correlated with current events, identified FIMI aimed at interfering in key events such as elections or opportunistically exploiting breaking news events, including EU political events.

Among the 86 identified cases, 52 involved at least one known Information Manipulation Set (IMS) with Matryoshka (18 cases) being the most active. Doppelgänger (6), Storm-1516 (5) and Russian Foundation to Battle Injustice (4) were involved to a lesser extent. In 19 cases, the Portal Kombat infrastructure was used to amplify content[338] [339]. In four additional cases, the case was imputed to another known IMS.

Fig. 37 - Identified Russia-aligned FIMI in the EU.
Source: EEAS STRATCOM / ENISA



Approximately a quarter of the documented FIMI content focused on degrading the Union through negative narratives. High-ranking officials such as the President of the European Commission and the High Representative for Foreign Affairs and Security Policy and the Vice-President of the European Commission were frequently targeted ahead of key strategic events[340] or discredited through the circulation of out of context pictures and quotes, disseminated via inauthentic articles and amplified by un-associated accounts[341], as well as statements from state-controlled Russian media[342].

Standing out in terms of both the frequency and diversity of operations against their public institutions, **France, Germany and Poland** are frequently targeted with narratives aimed at discrediting their government, military and intelligence services, often accusing them of destabilisation efforts abroad or failing in their fundamental duties, such as protecting their own citizens[343]. Police departments[344] and public media outlets[345] are commonly at the centre of Matryoshka campaigns, where they are either impersonated or misattributed to

[338] https://ghostarchive.org/archive/ODntI
[339] https://archive.ph/Vbtqp
[340] https://ghostarchive.org/archive/cp9Yu
[341] https://archive.ph/G3tvv
[342] https://archive.ph/OsOUT
[343] https://ghostarchive.org/archive/zTTNz
[344] https://ghostarchive.org/archive/WTwtq
[345] https://ghostarchive.org/archive/565Vk

increase legitimacy of false narratives. The intensity of attacks against public institutions tended to **increase around and during election periods or important political events**.

Doppelgänger, a major and long-running IMS, recently imputed to Struktura and Social Design Agency, and reportedly directly funded by the Russian state[346] was seen to be particularly targeting French, German and Polish national audiences and public institutions, as well as the Union, most notably through inauthentic articles conveying anti-EU sentiments, especially in the context of Russia's war of aggression against Ukraine. With an initial focus on impersonating Western news outlets and government websites, Doppelgänger has evolved into a multi-layered operation, reportedly deploying large networks of fake domains impersonating legitimate outlets designed to manipulate platform algorithms, running sponsored ads on Meta[347] to drive traffic to its deceptive sites and relying on large-scale Coordinated Inauthentic Behaviour (CIB) networks to ensure widespread distribution. Over time, the campaign has shown resilience, by refining its techniques and adapting to takedowns by hosting providers and social media platforms by re-registering websites under different Top-Level Domains (TLDs), migrating to different hosting providers and using disposable social media accounts to amplify content[348]. In December 2024, Doppelgänger-associated entities and individuals were sanctioned by the EU[349], the UK[350] and the US[351].

Notably known for its videos impersonating EU institutions such as the Parliament and the Commission, EU MSs public institutions within the security sector[352] and public media outlets, Matryoshka[353] [354] was reported to be using AI-assisted voice cloning to increase perceived legitimacy of the impersonation videos[355], with June 2025 marking the first iteration cloning of the voice an EU official[356]. The videos are amplified on X and Bluesky through two sets of coordinated inauthentic accounts (CIBs), the first set known as 'seeder' accounts posting the videos, further shared through a larger set of accounts known as 'amplifiers'. While targeting similar audiences as Doppelgänger, Matryoshka impersonates French and German public institutions with narratives addressing broader audiences with misleading narratives[357] [358] [359]. The IMS strategically exploits narratives during major events such as election campaign seasons in countries such as Poland and Moldova. Matryoshka has reportedly funnelled substantial operational resources towards Moldova[360].

Storm-1516[361] [362] operates a growing network of at least 230 inauthentic websites to publish inauthentic articles in the English, French and German languages and display visual features mimicking Western media outlets. These inauthentic websites, as well as X accounts, are used to strategically launder information, with some of them identified for their repeated involvement in FIMI operations including publication of fake investigations, social media posts and videos. Over the reporting period, Storm-1516 notably focused its actions on the German legislative elections, publishing multiple narratives questioning the integrity of the elections[363]. Investigations show the involvement of individuals and organisations close to the Russian government behind the operations carried out by Storm-1516[364]. Known for its overlap in amplification patterns with Storm-1516, The Russian Foundation to Battle Injustice often publishes content mostly in English, German and French, such as inauthentic articles, which is then laundered and amplified across various

[346] https://mpf.se/psychological-defence-agency/publications/archive/2025-05-15-beyond-operation-doppelganger-a-capability-assessment-of-the-social-design-agency
[347] https://www.whattofix.tech/publications/bankrolling-sanctioned-entities/
[348] https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en
[349] https://www.consilium.europa.eu/en/press/press-releases/2024/12/16/russian-hybrid-threats-eu-agrees-first-listings-in-response-to-destabilising-activities-against-the-eu-its-member-states-and-partners/
[350] https://www.gov.uk/government/news/uk-sanctions-putins-interference-actors
[351] https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence
[352] https://ghostarchive.org/archive/WTwtq
[353] https://www.sgdsn.gouv.fr/files/files/20240611_NP_SGDSN_VIGINUM_Matriochka_EN_VF.pdf
[354] https://checkfirst.network/operation-overload-how-pro-russian-actors-flood-newsrooms-with-fake-content-and-seek-to-divert-their-efforts/
[355] https://ghostarchive.org/archive/KBPC2
[356] https://ghostarchive.org/archive/iSaX1
[357] https://ghostarchive.org/archive/SYeXu
[358] https://archive.ph/04Tvx
[359] https://archive.ph/L7wzM
[360] https://archive.ph/7GC44
[361] https://euvsdisinfo.eu/building-a-false-facade/
[362] https://www.recordedfuture.com/research/russia-linked-copycop-uses-llms-to-weaponize-influence-content-at-scale
[363] https://archive.ph/8y74o
[364] https://www.sgdsn.gouv.fr/files/files/Publications/20250507_TLP-CLEAR_NP_SGDSN_VIGINUM_Technical%20report_Storm-1516.pdf

platforms, mostly X, Bluesky and, in some cases, Reddit[365]. Identified content focuses on portraying the EU as a hegemonic power interfering in Member States politics, particularly undermining their democratic processes by alleging that the EU is persecuting opposition parties and even attempting to ban them or violating human rights[366].

8.1.2 Other Information Manipulation Sets

In August 2024, an open-source publication documented an **information operation aligned with China' strategic interests** through social networks[367]. Named Green Cicada Network, this campaign operated a botnet comprised of 5 000 AI-operated accounts on X, notably accounts purportedly originating from the EU, to target Western Europe audiences. This campaign is assessed as being carried out by Yukuo Cen (aka cenyk1230), a Chinese AI researcher employed at Zhipu AI, a company allegedly tied to the People's Liberation Army and Chinese intelligence services. Of interest is **the convergence, mutual learning and increasing alignment between Chinese and Russian IMS, and the adoption of Russian FIMI disinformation TTPs by China**, leading to overlapping narratives and coordinated influence operations where Russian and Chinese networks mutually amplify content, to notably spread anti-Western narratives – notably when Chinese state-controlled media offer a platform to sanctioned Russian outlets[368] [369]. January 2025 saw the targeting of Spain in the China-aligned Spamouflage operation since December 2024, leveraging the floods in Valencia, Spain, to call for the overthrow of the Spanish government[370].

Also identified over the reporting period were **Iran-aligned** influence operations pertaining to the participation of Israel in the **Olympics**[371] [372], as well as **operation A2Z**, a campaign sharing similarities with VIGINUM's (U) notorious BIG, **associated to the Baku Initiative Group (BIG)**[373] [374], notably targeting audiences in France, Italy, Poland and Germany[375].

8.2 KEY FIMI TRENDS

8.2.1 Tactics, Techniques and Procedures (TTPs)

FIMI activities targeting EU entities and public institutions in Member States leverage a wide array of techniques as defined by the DISARM framework[376].

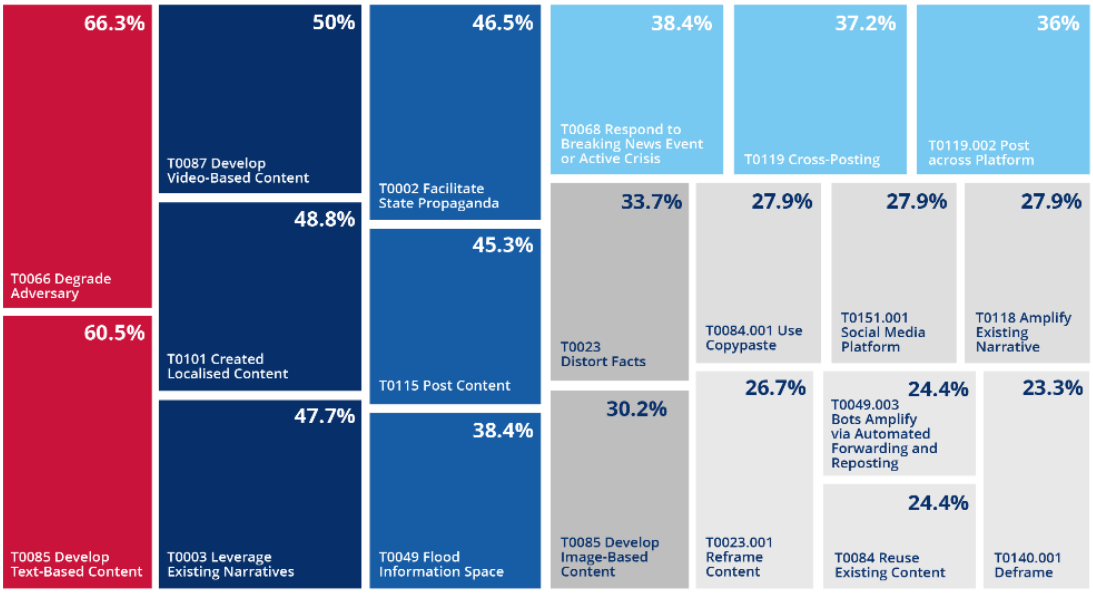
- **The use of Inauthentic news articles**. This was the most common type of content to convey narratives against EU entities and public institutions in EU MSs (T0085 Develop Text-Based Content, T0140.001 Defame, T0066 Degrade Adversary). Articles are often transformed into social media posts either by taking the headline or a text extract to be amplified across platforms (T0084 Reuse Existing Content).
- **Fabricated investigations.** EU entities and public institutions in EU MSs were the subject of fabricated investigations (T0085 Develop Text-Based Content, T0023.001 Reframe Context). Often originated by the Russian Foundation to Battle Injustice, the content was laundered through inauthentic websites and unattributed channels posting across platforms (T0119 Cross-Posting; 37.2%). It was translated and shared across multiple inauthentic websites and accounts on X (T0003 Leverage Existing Narratives, T0049.003 Bots Amplify via Automated Forwarding and Reposting).
- **Decontextualised quotes and images**. FIMI actors aimed to discredit EU officials by decontextualising and reframing statements, image or previously published content (T0023.001 Reframe Context). While the

[365] https://web.archive.org/web/20250708220546/https://fondfbr.ru/stati/sindikat-ambrozia/
[366] https://archive.ph/k3lSh
[367] https://connect.cybercx.com.au/Intelligence-Update-CCX-IU-2024-004
[368] https://www.japantimes.co.jp/commentary/2024/12/25/world/russia-china-disinformation-online/
[369] https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf
[370] https://22006778.fs1.hubspotusercontent-na1.net/hubfs/22006778/atlas-highlights-china.pdf
[371] https://www.ic3.gov/CSA/2024/241030.pdf
[372] https://therecord.media/iran-cyber-group-targeted-paris-olympics-israel
[373] https://www.france.fr/en/article/french-overseas-territories/
[374] https://www.sgdsn.gouv.fr/publications/un-notorious-big-une-campagne-numerique-de-manipulation-de-linformation-ciblant-les
[375] https://cdn.openai.com/threat-intelligence-reports/influence-and-cyber-operations-an-update_October-2024.pdf
[376] https://www.disarm.foundation/framework

original content may be authentic, it is reframed to better fit FIMI narratives and disseminated by unattributed channels (T0049.003 Bots Amplify via Automated Forwarding and Reposting (T0140.001 Defame).

- **False documents.** These were used to target mostly public institutions in EU MSs through misattribution. The documents allegedly 'leaked' are disseminated on social media through unattributed channels. (T0003 Leverage Existing Narratives).
- **Amplification by state-controlled channels**. Official Russian and Belarusian state-controlled channels published content aiming to discredit the EU on multiple occasions, which was then disseminated in various languages by unattributed channels and at times the Portal Kombat infrastructure. (T0023 Distort Facts, T0140.001 Defame).
- **Artificial Intelligence**. Over the past year, FIMI actors increasingly relied on Artificial Intelligence (AI) to facilitate their efforts, with 14.3% of recorded cases targeting EU entities and public institutions in EU MSs.

Fig. 38 - Identified Russia aligned FIMI TTPs (DISARM).
Source: EEAS STARTCOM



The TTPs shown in the graph hereunder are tagged according to the DISARM framework[377] and give a general overview on the type of behaviour and assessed motives of the IMS.

8.2.2 Exploitation of strategic events

Over the reporting period, 72.5% of cases of FIMI campaigns targeting Union entities and EU public institutions either targeted an event or opportunistically exploited current news.

European institutions were targeted during the Polish elections mostly by the Doppelgänger campaign; this activity was complemented by Russian and Belarusian media. The IMS focused its efforts on targeting EU institutions, aiming to undermine key policies, particularly the Green Deal, while portraying Brussels as interfering in Poland's sovereign decision-making[378] [379]. Russian and Belarusian media activity focused on accusing the EU, especially its Commission and Parliament, of interfering in the Polish elections[380] [381].

[377] https://github.com/VIGINUM-FR/DISARM-FR
[378] https://archive.ph/LhoSV
[379] https://archive.ph/kbgYh
[380] https://ghostarchive.org/archive/QrxCh
[381] https://archive.ph/ynXr9

In the context of the Romanian elections, FIMI activities targeting EU entities focused on accusing them of attempting to manipulate the electoral outcome. Russian state-controlled media outlets and official government channels played a key role in shaping and disseminating the core narratives[382], which were later adapted and amplified through IMS, notably Doppelgänger and Portal Kombat. For instance, the Russian Foreign Intelligence Services published a press release accusing the President of the European Commission of pressuring Romanian authorities to arrest a far-right politician[383], which was reshared by Russian and Belarusian state-controlled media as well as the Portal Kombat infrastructure[384] [385].

During the Moldovan Presidential elections and as the vote also included a referendum on EU accession, EU entities were particularly targeted. Russian FIMI activities leveraged themes of interference, portraying the EU as hegemonic and tyrannical. It particularly exploited topics linked to LGBTIQ+ rights to further these narratives. Various behavioural patterns were leveraged in these incidents, including videos impersonating the President of the European Commission and its Vice-President, and manipulated quotes of the EU Ambassador to Moldova[386] [387] [388] [389] [390].

Besides elections, a wide array of events was exploited to further their narratives and degrade Union entities and public institutions in EU MSs as illustrated by a video demanding the replacement of the EU ambassador to Niger, accused of misuse of funds and destabilisation following an EU announcement of €4.5 million in aid to the flood ridden Sahel and Lake Chad regions[391]. Similarly, Matryoshka leveraged the April 2025 European power outage blaming it on EU sanctions on Russia and accusing the President of the European Commission of blaming it on Russia[392].

[382] https://archive.ph/VgVN0
[383] https://archive.ph/VgVN0
[384] https://archive.ph/kGpGj
[385] https://archive.ph/kLUk9
[386] https://web.archive.org/web/20250529083251/
[387] https://twitter.com/jelefrancois1/status/1928006613262090257
[388] https://archive.ph/61O4d
[389] https://archive.ph/5ZT1F
[390] https://archive.ph/5X5Dh
[391] https://ghostarchive.org/archive/m4DZg
[392] https://archive.ph/gGGA9

9. HACKTIVISM

Despite their minimal impact and low-advanced attacks, hacktivist groups remained the most active threat against EU MSs, with claimed attacks continuously increasing over the reporting period, reaching **79% of total incidents.**

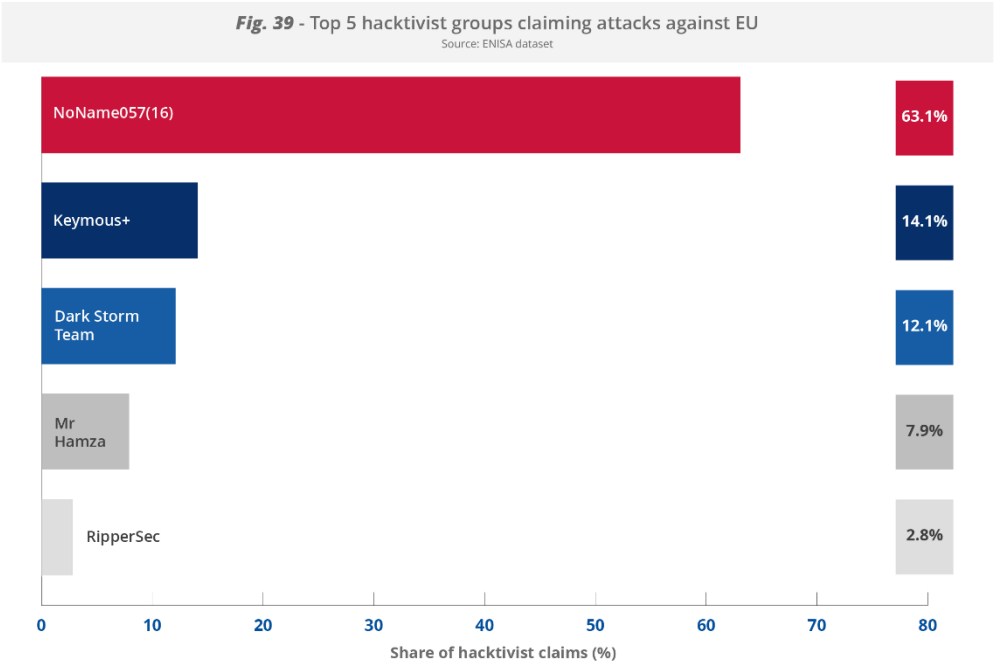
DDoS attacks against the websites of EU MSs constituted 91.5 % of incidents, with exceptionally low instances of claimed intrusions (5.1%), and data breaches (3.4%). Of particular interest in addition to the increased activity against EU MSs by pro-Russia hacktivist groups is the prevalence of pro-Palestine groups, likely related to announcements of an increasing number of alliances.

9.1 KEY HACKTIVISM THREATS

At least **88 hacktivist groups** claimed they targeted EU MSs organisations. Pro-Russia nexus hacktivist groups remain prevalent, with 63.1% of attacks claimed by NoName057(16), followed by Keymous+ (14.1%), Dark Storm Team (12.1%), Mr Hamza (7.9%), and RipperSec (2.8%).

While the core hacktivist threat landscape is shaped by a few hacktivist groups, it is also populated by **short-lived campaigns triggered by specific events** with hacktivist groups claiming attacks and then disappearing, with claimed activities ranging from a few days to a few weeks.

Fig. 39 - Top 5 hacktivist groups claiming attacks against EU
Source: ENISA dataset



The tempo of activity across the five most active hacktivist groups indicated **differing operational patterns.**

Pro-Russia **NoName057**(16) sustained the highest operational tempo, with continuous campaigns throughout the reporting period and a clear ability to **mobilise rapidly across multiple EU states**, likely due to their crowd-sourced model operationalised through the DDoSia platform. The Dark Storm Team also demonstrated a steady tempo, with frequent medium-scale operations, while Keymous+ displayed a spike-driven tempo, characterised by bursts of activity in specific quarters, notably against France and Estonia, pointing to possible ad-hoc mobilisation. Mr Hamza's activity remained episodic, with periods of large-scale attacks followed by lulls. Finally, RipperSec exhibited a low but increasing tempo from September 2024 onwards.

NoName057(16) claims particularly pertained to the targeting of Italy, France and Poland, alongside Lithuania and Germany. This illustrates a particular emphasis on EU MSs possibly being perceived as threats to Russia in that country's ongoing war of aggression against Ukraine. NoName057(16) reportedly focused on entities operating in the public administration with sustained targeting of ministries, parliamentary websites and local municipalities as well as finance, with a focus on banks and payment service providers, and transport, notably air and rail transport websites, with the occasional targeting of telecoms and hosting services. NoName057(16)'s activities were highly **driven by geopolitical events, including declarations of support for Ukraine by EU MSs and Union entities, as well as socio-political situations at the EU level.** These are illustrated by their DDoS attacks against the websites of Europol and the European Parliament in response to EU foreign policy actions in September 2024[393], and the targeting of Belgian electoral infrastructure for seven consecutive days, in retaliation for that EU MS's commitment to supply military equipment to Ukraine[394] [395].

Assessed to be a 'for-hire' opportunistic group originating from North Africa[396], **Keymous+** demonstrated a focus on France and Estonia, with activities in Belgium, Denmark and Germany. Most claims were related to public administration, mostly municipal and regional government portals, followed by finance, notably insurance firms and regional banks, digital infrastructure, including domain registrars and cloud providers, education, and media/entertainment.

The pro-Palestine anti-Israel **Dark Storm Team** primarily targeted Poland and Finland, followed by France, Lithuania and Germany. The group's campaigns were particularly prevalent against the EU public administration sector, followed by transport, finance and media/entertainment and manufacturing. The Dark Storm Team focused heavily on Ministries of defence and Ministries of foreign affairs, aviation and airport services, and news outlets.

The pro-Palestine anti-Israel **Mr Hamza** claimed attacks against France, Spain, Germany, Lithuania and Belgium, with attacks focused on public administration, with a notable targeting of the manufacturing sector. The group was seen to increase its activities after Q4 2024, through their participation in the Holy League alliance, which reportedly gathered pro-Russia and pro-Palestine groups[397] [398] [399] [400] [401] [402]. Between February and March 2025, Mr Hamza was particularly involved in coordinated campaigns, including #op_france[403], #op_italia, #opromania, #opbelgium, and #opnato[404] [405] [406].

The pro-Russia **Rippersec**, while relatively less active, demonstrated a slow but steady increase in activity against EU MSs throughout the reporting period. This group appeared to specifically target the public administration and media/entertainment sectors, followed by transport, with a claimed intent to target operational technology (OT).

THE OVERALL IMPACT OF DDOS ACTIVITIES REMAINED MARGINAL.
For each most active hacktivist group, analysis shows that explicitly confirmed disruptions are quite limited, with Keymous+ and Mr Hamza appearing slightly more disruptive with approximately 1.5% of attacks resulting in websites slowdowns and/or disruptions. Interestingly, while the most prolific in terms of volume, NoName057(16) activities led to almost no confirmed outages, further corroborating the hypothesis of an information operation aspect to activities carried out by this group.

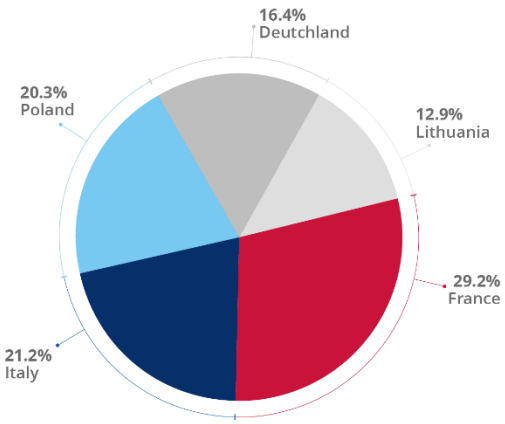
[393] https://www.europarl.europa.eu/news/en/press-room/20240913IPR23906/meps-ukraine-must-be-able-to-strike-legitimate-military-targets-in-russia
[394] https://www.vrt.be/vrtnws/en/2024/10/07/pro-russian-group-launches-cyber-attack-on-belgian-cities-and-pr/
[395] https://x.com/Noname05716/status/1843313547381710985
[396] https://www.radware.com/blog/threat-intelligence/keymous-plus-a-new-hacktivist-collective-or-a-ddos-as-a-service-brand/
[397] https://t.me/blackopmrhamza/681
[398] https://t.me/blackopmrhamza/694
[399] https://t.me/blackopmrhamza2/113
[400] https://t.me/mrhamzaofficiel/429
[401] https://t.me/mrhamzaofficiel/754
[402] https://t.me/blackopmrhamza/508
[403] https://t.me/blackopmrhamza2
[404] https://t.me/blackopmrhamza2/37
[405] https://t.me/blackopmrhamza2/403?single
[406] https://t.me/blackopmrhamza2/408

9.2 HACKTIVISM GEOGRAPHICAL TARGETING

Over the reporting period, hacktivism-related activities in the EU mostly targeted organisations in **France, Italy, Poland, Germany and Lithuania.**

While not all of them were necessarily linked with hacktivism, **France** was reportedly the second most targeted country in the world by DDoS attacks in 2023[407]. **Peaks** in activity identified in this EU MS were **congruent with potentially divisive issues relevant to the political and societal national context, as well as declarations of support for Ukraine**[408] [409], most notably conducted under the #OPFrance banner [410] [411] [412] [413] [414] [415]. Almost half of hacktivist activities recorded against France were carried out by NoName057(16), followed by Keymous+, Dark Storm Team, Mr Hamza, and RipperSec. While all were seen to be focusing on the public administration sector, Keymous+ appeared to primarily target the finance sector, and NoName057(16) and Keymous+ both claimed attacks against the media/entertainment sector. It is possible the targeting of France by self-proclaimed pro-Russia and pro-Palestine hacktivist groups stems from the fact that this EU MS is one of the most vocal against Russia's war of aggression in Ukraine and the Hamas/Israel conflict, and is also a permanent Member of the United Nations Security Council.

Fig. 40 - Top 5 EU MS reportedly targeted by hacktivist groups.
Source: ENISA dataset



The top five hacktivist groups targeting Italy included NoName057(16), Dark Storm Team, DXPLOIT, Mr Hamza and Alixsec, notably under the #OPItaly banner which was increasingly used in Q1 2025. While attacks targeting public administration represented X% of the claimed activities of these groups[416] [417] [418], NoName057(16) and Dark Storm Team and DXPLOIT were observed targeting the transport sector. It may be noted that **Italy reportedly faced increased targeting of OT systems by Z-PENTEST-ALLIANCE from Q4 2024 onwards**.

Poland was, in particular, targeted by NoName057(16), Dark Storm Team, SERVER KILLERS, OverFlame, and Keymous+. More than half of hacktivist claims pertained to the public administration sector, followed by the finance sector, transport, and energy verticals. Of note, **the energy sector in Poland appears to be of particular interest to NoName057(16) and OverFlame**, both part of the Z-PENTEST-ALLIANCE, which demonstrated intent and capability to target OT systems.

In Germany, most active groups included NoName057(16), Keymous+, Dark Storm Team, Mr Hamza and Mysterious Team Bangladesh. Offensive cyber activities targeting the public administration remained prevalent, with one outlier identified as **Mysterious Team Bangladesh seemingly focused on targeting the transport and energy sectors**. Of interest also is the sustained targeting of finance and manufacturing entities by NoName057(16).

[407] https://www.f5.com/labs/articles/threat-intelligence/2024-ddos-attack-trends
[408] https://www.connexionfrance.com/news/strikes-in-france-in-march-2025-and-how-you-may-be-impacted/710661
[409] https://apnews.com/article/france-politics-prime-minister-bayrou-budget-confidence-ed939b7afd004e50a3831e75db318454
[410] https://t.me/c/2537471062/86
[411] https://t.me/blackopmrhamza/589
[412] https://t.me/mrhamzaofficiel/307
[413] https://t.me/KeymousTeam/580?single
[414] https://t.me/KeymousTeam/953
[415] https://t.me/c/2602447593/158
[416] https://t.me/c/2592664591/339
[417] https://t.me/c/2592664591/340
[418] https://t.me/Darkstormbackup2/294

Accounting for approximately 70% of the claims against Lithuania, NoName057(16) was followed by Dark Storm Team, Mr Hamza, OverFlame, and Z-PENTEST-ALLIANCE. While NoName057(16), Dark Storm Team and Mr Hamza demonstrated a focus on targeting the public administration and transport sectors, NoName057(16) was also observed targeting the finance vertical.

A more granular analysis of our dataset shows some level of focus against specific EU MSs, with clear outliers being the **activities of Keymous+ in Estonia and France,** and **Dark Storm Team activities against Poland and Finland**. While it is not possible to establish a clear connection, it is plausible some hacktivist groups might have specific geographic assignments to support and/or complement activities against specific EU MSs.

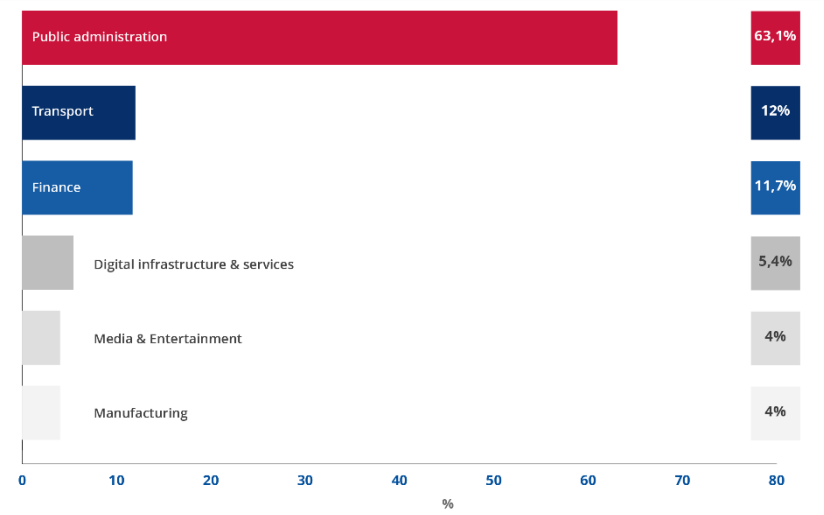
As previously mentioned, **peaks** of hacktivist activity are typically **observed following announcements related to Ukraine**[419] [420] [421], as notably exemplified by the launch of the #OPBelgium campaign following Belgium's announcement of €1B in military aid[422] [423] [424]. A few outliers further illustrating this observation were identified in ENISA's dataset. Between the end of April and May 2025, Anonymous VNLBN claimed at least 27 attacks against France, following announcements of support for Ukraine and the freezing of Russian assets[425] [426]. Fredens of Security's targeting of Italy, Germany, Denmark and Poland between 12 and 15 December 2024 followed declarations of assistance and equipment deliveries to Ukraine[427] [428] [429]. The targeting of Belgium by INDOHAXSEC TEAM from 10 December to 12 December 2024 may be viewed in the context of the European Council's approval of the second payment under the EU's Ukraine Facility[430]. It may be noted that these groups were only active for these very short-lived, highly focused operations.

Finally, **EU MSs electoral processes** over the reporting period were particularly targeted by hacktivist-led DDoS claims[431] [432] [433].

9.3 HACKTIVISM SECTORIAL TARGETING

Across the EU, targeting patterns reveal both common sectorial focuses and country-specific nuances, with **public administration, finance, transport and digital infrastructure remaining the prime targets across all EU MSs**. The targeting of manufacturing and energy sectors is prevalent in Poland, Czechia and Romania, all three being heavily involved in supply-chain support for Ukraine. Over the reporting period, the most impacted sectors by hacktivist activities in the EU included public administration (63.1%), transport (12%), finance (11.7%), digital infrastructure (5.4%), and manufacturing and media/entertainment (4% each).

Fig. 41 - Hacktivist claims against EU sectors
Source: ENISA dataset



[419] https://t.me/noname05716_reborn2/206
[420] https://t.me/c/2890597202/181
[421] https://t.me/Darkstormbackup2/276
[422] https://kyivindependent.com/ukraine-belgium-sign-long-term-security-deal/
[423] https://t.me/KeymousTeam/406
[424] https://t.me/c/1914467285/8098
[425] https://www.lemonde.fr/en/international/article/2025/04/18/war-in-ukraine-first-talks-between-americans-ukrainians-and-europeans-in-paris-yield-no-real-breakthrough_6740379_4.html
[426] https://www.reuters.com/world/europe/eu-countries-adopt-plan-use-frozen-russian-assets-ukraines-defence-2024-05-21/
[427] https://www.reuters.com/world/europe/italy-approve-more-military-aid-ukraine-this-month-sources-say-2024-12-03/
[428] https://apnews.com/article/russia-ukraine-war-f16-denmark-86c2d6631869cc8f5217482e22bf52d8
[429] https://www.reuters.com/world/europe/norway-send-f-35-fighter-jets-air-defence-systems-poland-2024-12-02/
[430] https://www.consilium.europa.eu/en/press/press-releases/2024/12/09/council-approves-second-payment-of-over-42-billion-under-the-ukraine-facility/
[431] https://t.me/noname05716engver/1035
[432] https://t.me/nnm057_16/6239
[433] https://t.me/c/2442953840/142

Consistently targeted over the reporting period and across all EU MSs, public administration was the most targeted sector, specifically **governmental websites** (51.5%) and **municipalities** (34%). The most impacted EU MSs overall were Italy, France, Spain, Poland and Germany, and the most active hacktivist groups targeting this sector were NoName057(16), Dark Storm Team, Mr Hamza, Keymous+ and Mysterious Team Bangladesh. As an EU MS supporting Ukraine and the host country of several EU and international organisations, the **targeting of public administration in Belgium remains prevalent**, with incidents related to this sector representing a disproportionately high share of Belgium's overall targeting, often accounting for more than half of all incidents. This iteration also saw an **increased targeting of intelligence and security services**, with incidents concentrated in a few EU Member States in Eastern and Northern Europe where law enforcement has taken high-profile actions against hacktivist groups. These attacks tend to occur as retaliatory spikes rather than sustained campaigns, reflecting hacktivist attempts to signal against domestic security institutions.

Accounting for 6.1% of all recorded hacktivist-led incidents, the transport sector was particularly targeted in Poland, Germany and Italy, with a prevalence of attacks on **air and rail transport entities.** NoName057(16), Dark Storm Team, Mr Hamza, Keymous+ and RipperSec were reportedly the most active groups in targeting this sector.

The same group of hacktivists were also recorded targeting the finance sector, with a focus on the **public-facing portals of banks**, particularly in Italy, Spain and France.

While less prevalent and quite volatile from one month to the next, the targeting of digital infrastructure by hacktivist groups is of particular concern due to its potential for systemic, cross-border impact. This sector was seen targeted by NoName057(16), RipperSec, Dark Storm Team, Keymous+ and Mr Hamza, with the most targeted EU MSs being Germany, the Netherlands and France.

Interestingly, the manufacturing sector, especially **defence-related** and **automotive-related** entities, were seen particularly targeted by RipperSec, followed by NoName057(16), Dark Storm Team, Keymous+ and Mr Hamza; these attacks were most prevalent in Germany and Poland.

Finally, the French and German media/entertainment sector, specifically **news outlets and broadcasters**, were in particular targeted over the reporting period, with the most active groups including Mr Hamza, NoName057(16), Dark Storm Team, Keymous+ and RipperSec.

9.4 KEY HACKTIVISM TRENDS

9.4.1 Tactics, Techniques and Procedures (TTPs)

In addition to adopting **allegedly advanced TTPs** for DDoS attacks, hacktivist groups were increasingly reported leveraging **ransomware**, as well as **targeting OT**.

Multiple open-source reports notably documented the use of carpet bombing[434] or routers leveraging as well as AI to increase intensity and the potential impact of their DDoS attacks. According to a report by Netscout related to the first semester of 2024, bot-infected devices rose by 50%, largely due to the emergence of the Zergeca botnet alongside the evolving DDoSia botnet used by NoName057(16), which employs DNS over HTTPS (DoH) for Command and Control (C2) activities. **Leveraging or transitioning to ransomware** is particularly prevalent among pro-Russia groups, as illustrated by the launch of their own RaaS by the CyberVolk's, Azzasec, Funksec and Lapsus$ groups[435] [436] [437]. KillSecurity, originally a pro-Russia hacktivist group aligned with Anonymous, transitioned into a notable player in the ransomware landscape following the

[434] https://nsfocusglobal.com/a-deep-dive-into-ddos-carpet-bombing-attacks/
[435] https://www.infosecurity-magazine.com/news-features/why-hacktivists-joining-ransomware/
[436] https://www.sentinelone.com/labs/cybervolk-a-deep-dive-into-the-hacktivists-tools-and-ransomware-fueling-pro-russian-cyber-attacks/
[437] https://www.rapid7.com/blog/post/2024/10/03/ransomware-groups-demystified-cybervolk-ransomware/

launch of its RaaS platform in June 2024[438], and has targeted multiple EU MSs ever since, with increased activity reported in April 2025.

Hacktivist groups continued **displaying intent, capacity and opportunity to target OT systems**, as illustrated by **Z-PENTEST-ALLIANCE's** claimed targeting of Internet-accessible OT management interfaces operated in the energy and water management sectors[439], notably in Italy[440] [441] [442] [443] [444] [445] [446], Czechia[447], Lithuania[448] [449] [450] [451] , Poland[452], Portugal[453], the Netherlands[454] and Spain[455] [456] . While these attacks reportedly did not result in significant operational impact, the sharing of videos showing Z-PENTEST-ALLIANCE operators tampering with OT systems is assessed to aim at amplifying the threat for psychological impact. Z-PENTEST-ALLIANCE reportedly became the leading hacktivist group targeting critical infrastructure, with a focus on energy infrastructure in the EU, with Italy documented as the most frequently targeted EU MS in OT attacks by hacktivists, followed by the Czechia, France, and Spain[457]. Z-PENTEST-ALLIANCE has increasingly proclaimed its intention to target OT since Q1 2025, notably through their alleged association to Russia-nexus intrusion set Sandworm. While Sandworm was previously documented operating the Cyber Army of Russia Reborn (CARR) faketivist group, this claim cannot be verified and is assessed as doubtful at the time of reporting. Emerging in June 2025, the **Infrastructure Destruction Squad (IDS**) reportedly developed the VoltRuptor ICS specific malware, reportedly offering advanced multi-protocol support and advanced persistence and anti-forensics capabilities to enable cross-platform operations. On 30, June 2025, IDS reportedly compromised an Italian smart building automation company. Of note VoltRuptor is documented as being available for sale on the dark web. As this threat is too recent to assess, the leveraging of the IDS persona by a Russia-nexus intrusion set is a realistic working hypothesis.

9.4.2 Evolution of the ecosystem

In addition to previously mentioned hacktivist activities overlapping with cybercrime TTPs and ecosystems, **newly formed alliances** gathering together hacktivist groups with seemingly distinct ideologies were announced during the reporting period.

Further complementing bilateral associations[458] [459] [460] [461] , highlights of this increasing trend include the formation of **The Holy League**, announced in July 2024[462], reportedly gathering 70 groups, including pro-Russia NoName057(16), and pro-Palestine hacktivists, to target Ukraine, Israel and countries perceived as supporting Ukraine and Israel, as well as NATO Allies, including EU MSs. The Holy League notably targeted Spain in retaliation for the arrest of individuals linked to NoName057(16)'s DDoSia, which led to NoName057(16)'s claimed DDoS attacks against multiple Israeli entities presented as a token of appreciation for Holy League's attacks on Spain[463] [464]. The Holy League was also observed carrying out attacks against the

[438] https://thecyberexpress.com/killsec-launches-raas-program/
[439] https://cyble.com/blog/russian-hacktivists-target-energy-and-water-infrastructure/
[440] https://t.me/Z_Pentest_Beograd/523
[441] https://t.me/Z_Pentest_Beograd/527
[442] https://t.me/Z_alliance_ru/273
[443] https://t.me/Z_alliance_ru/531
[444] https://t.me/Z_alliance_ru/303
[445] https://t.me/Sector08/227
[446] https://t.me/musicarusaesp/5967
[447] https://t.me/Z_alliance_ru/572
[448] https://t.me/Z_alliance_ru/802
[449] https://t.me/Z_alliance_ru/706
[450] https://t.me/Z_alliance_ru/639
[451] https://t.me/Z_alliance_ru/623
[452] https://cyberdefence24.pl/cyberbezpieczenstwo/zaatakowano-polski-szpital-i-oczyszczalnie-kierunek-rosyjski#google_vignette
[453] https://t.me/Z_alliance_ru/304
[454] https://t.me/Z_Pentest_Beograd/531
[455] https://dailydarkweb.net/noname05716targets-water-supply-system-in-spain/
[456] https://t.me/Sector08/197
[457] https://cyble.com/blog/hacktivists-attacks-on-critical-infrastructure/
[458] https://t.me/Darkstormbackup2/33
[459] https://t.me/dakrstormteam21/8
[460] https://x.com/FalconFeedsio/status/1881649397936906529
[461] https://x.com/FalconFeedsio/status/1878704845948944477
[462] https://t.me/h0lyleague
[463] https://x.com/Noname05716/status/1816839317509038248
[464] https://detect.fyi/cybervolks-ransomware-ad38134b1b0a

websites of French governmental entities and financial systems[465] [466] , in the context of the Ukrainian President's visit to Paris to hold a 'Trilateral meeting' with the French President and the then US president-elect.

The hacktivist ecosystem was also impacted by disruptions to their tools and means, as seen with Telegram's increased cooperation with law enforcement, operationalised through the ban or take downs of more than 60 hacktivist-linked aliases in Q1 2025[467]. This notably resulted in hacktivist groups migrating to private Telegram rooms[468], X[469] [470], Element[471], and dark web forums[472]. In October 2024, Operation PowerOFF saw LEAs from 15 countries shut down 27 DDoS-for-hire platforms and arrest three administrators[473] [474] . This effort was expanded in February 2025, when a follow-up operation took six more DDoS-for-hire platforms offline and resulted in four arrests and nine domain seizures[475].

Examples of potential identity spoofing were also reported for the first time, with the claimed reappearance of pro-Russian Killmilk in May 2025[476] and cases of NoName057(16) impersonations with the use of ransomware decoys.

[465] https://cyble.com/blog/hacktivist-alliances-target-france/ 82 https://thecyberexpress.com/holy-league-hacktivists-uniting-against-france
[466] https://www.radware.com/security/threat-advisories-and-attack-reports/holy-league-a-unified-threat-against-western-nations/
[467] https://t.me/transparency
[468] https://t.me/c/2634086323
[469] https://x.com/Noname05716
[470] https://x.com/BlackMaskers0
[471] https://matrix.to/#/%23noname05716:matrix.org
[472] https://breachforums.st/Thread-Handala-New-Telegram-Channel?action=newpost
[473] https://www.europol.europa.eu/media-press/newsroom/news/lockbit-power-cut-four-new-arrests-and-financial-sanctions-against-affiliates
[474] https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-takes-down-two-largest-cybercrime-forums-in-world
[475] https://www.europol.europa.eu/media-press/newsroom/news/key-figures-behind-phobos-and-8base-ransomware-arrested-in-international-cybercrime-crackdown
[476] https://therecord.media/russian-hacker-group-killnet-returns-with-new-identity

10. TTPS & VULNERABILITIES

This section discusses the **technical coverage of adversary behaviours across the attack lifecycle**, mapped directly to MITRE ATT&CK IDs to provide an actionable foundation for SOC teams, detection engineers and threat hunters seeking to **prioritise coverage of common attacker techniques** and align their defensive strategies with relevant mitigations. The MITRE ATT&CK framework organises real-world observations into a matrix of tactics and techniques, offering detailed examples, detection guidance and mitigations[477]. The structured mapping highlights a strong defence-in-depth posture, with an emphasis on access controls, privilege restrictions, endpoint visibility and proactive detection of stealthy malicious behaviours.

10.1 OBSERVED TACTICS, TECHNIQUES & PROCEDURES (TTPS)

TTPs describe how adversaries operate, with Tactics describing their objectives, Techniques documenting the general methods they use and Procedures detailing the specific steps or tools they employ. Based on open-source reports, ENISA's dataset focuses heavily on **post-compromise activities**, particularly reconnaissance conducted by adversaries and methods to maintain access or execute malicious payloads after initial intrusion. Documented tactics associated with TA0040: Impact, TA0010: Exfiltration and TA0009: Collection are less frequent. At the technique level, the dataset **highlights the recurring tradecraft of adversaries around specific tactics.**

Figure 42 represents a clustered visualisation of common TTPs based on ENISA's dataset.

Fig. 42 - Most commonly seen TTPs.
Source: ENISA dataset

[477] https://attack.mitre.org/

A cluster appears around the **discovery techniques** (e.g., T1057 Process discovery, T1016 System network configuration discovery, T1082 System information discovery, T1083 File and directory discovery, T1135 Network share discovery), indicating they are frequently enumerated together under the discovery tactic, which is typical when adversaries inventory systems and networks.

A second cluster centres on **execution techniques** — notably the **command and scripting interpreter** family (T1059 and sub-techniques T1059.001/.003/.005) and related execution vectors (T1047 WMI, T1106 Native API, T1569.002 Service Execution, T1204.* User Execution). **Persistence** shows its own block (T1543.003 Windows Service, T1112 Modify Registry, T1547.* logon/registry autostart, T1136 Create Account, T1078.* Valid/Domain/Local Accounts), Persistence techniques like Windows Services (T1543.003), registry changes (T1112, T1547.) and account creation or abuse (T1136, T1078.) often appear together, showing how adversaries are able to layer multiple foothold methods. Smaller but coherent blocks appear for **Exfiltration** (T1041, T1048., T1052.001, T1567.) and **Impact** (T1485/86/89/90/91.001/1529).

A more detailed version of TTPs is available in the Appendix.

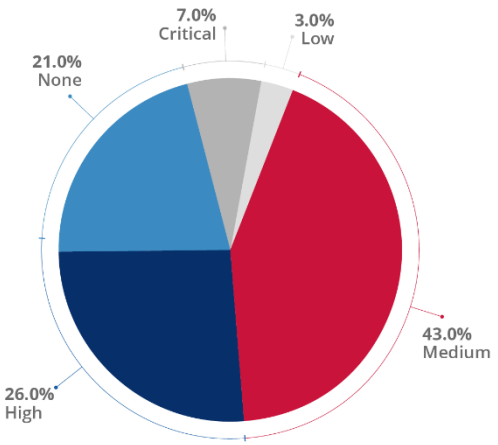
10.2 VULNERABILITIES

When documenting tactics, techniques and procedures (TTPs), it is important to recognise that vulnerabilities are part of the picture. Exploitation of vulnerabilities remains a prevalent intrusion vector (21.3%). Vulnerabilities are commonly assigned identifiers and, when included in TTP documentation and thoroughly documented, these connect adversary behaviour to the precise weaknesses they exploit. **Tracking vulnerabilities with the surrounding TTP context supports effective prioritisation**. By embedding vulnerabilities within the broader structure of TTPs, defenders gain both the technical detail needed for patching and the operational context needed to assess risk and allocate resources effectively.

In line with Coordinated Vulnerability Disclosure practices in the EU[478] and complementary to its role as a CVE Numbering Authority (CNA) [479], ENISA maintains the European Vulnerability Database (EUVD) [480] to further support the cybersecurity community by providing reliable and timely information related to vulnerabilities.

Overall, **42 595 new vulnerabilities** were disclosed over the reporting period — a **27% increase** from the previous year. A break-down of the vulnerabilities in the Common Vulnerability Scoring System (CVSS) shows that **7% were Critical, 26% High, 43% Medium and 3% Low**, while **21% remained unscored**, likely reflecting delays or gaps in CVSS assignments.

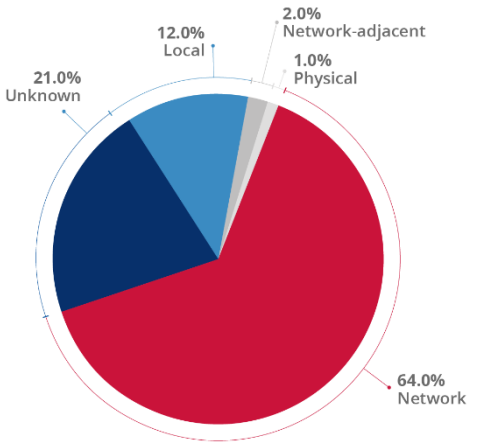
Fig. 43 - CVSS of vulnerabilities documented over the reporting period.
Source: EUVD



[478] https://csirtsnetwork.eu/homepage?tab=cvd
[479] https://www.enisa.europa.eu/topics/vulnerability-disclosure
[480] https://euvd.enisa.europa.eu/homepage

When considering the attack surface, **64% of documented vulnerabilities use the network as the attack vector**, in accordance with the definition of the CVSS Attack vector metric[481]. This underscores the potential risk of remote exploitation, especially for Internet-facing systems.

Fig. 44 - Attack vectors of all vulnerabilities documented over the reporting period.
Source: EUVD



Based on the Common Weakness Enumeration (CWE) list, 2024 most commonly saw the following top 25 weaknesses in hardware and software, that could have security ramifications.

Fig. 45, Top 25 commonly seen CWEs.
Source : CWE list

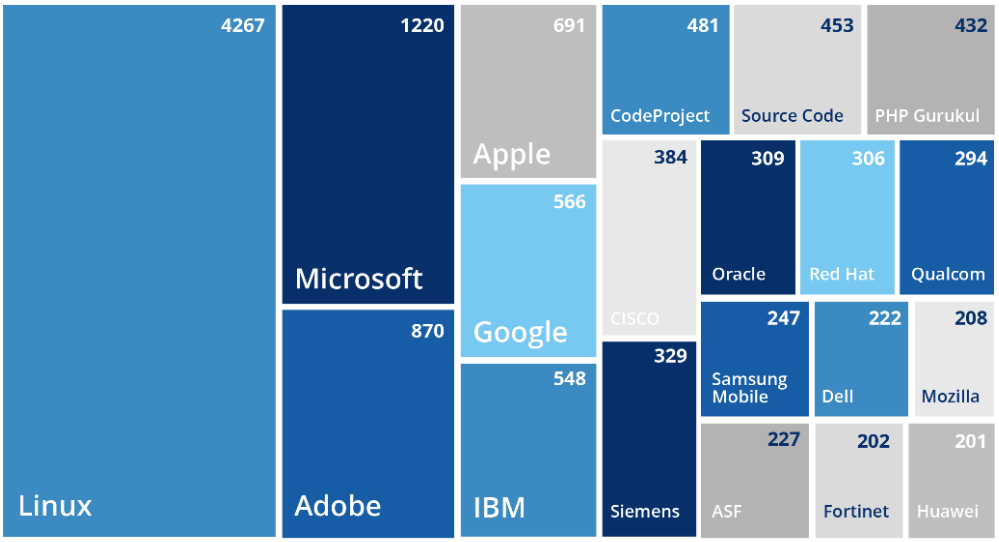
Rank	ID	Name	Score	CVEs in KEV	Rank Change vs. 2023
1	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	56,92	3	+1
2	CWE-787	Out-of-bounds Write	45,2	18	-1
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	35,88	4	0
4	CWE-352	Cross-Site Request Forgery (CSRF)	19,57	0	+5
5	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12,74	4	+3
6	CWE-125	Out-of-bounds Read	11,42	3	+1
7	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11,3	5	-2
8	CWE-416	Use After Free	10,19	5	-4
9	CWE-862	Missing Authorization	10,11	0	+2
10	CWE-434	Unrestricted Upload of File with Dangerous Type	10,03	0	0
11	CWE-94	Improper Control of Generation of Code ('Code Injection')	7,13	7	+12
12	CWE-20	Improper Input Validation	6,78	1	-6
13	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	6,74	4	+3
14	CWE-287	Improper Authentication	5,94	4	-1
15	CWE-269	Improper Privilege Management	5,22	0	+7
16	CWE-502	Deserialization of Untrusted Data	5,07	5	-1
17	CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	5,07	0	+13
18	CWE-863	Incorrect Authorization	4,05	2	+6

[481] https://www.first.org/cvss/specification-document

19	CWE-918	Server-Side Request Forgery (SSRF)	4,05	2	0
20	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	3,69	2	0
21	CWE-476	NULL Pointer Dereference	3,58	0	-9
22	CWE-798	Use of Hard-coded Credentials	3,46	4	+2
23	CWE-190	Integer Overflow or Wraparound	3,37	3	-9
24	CWE-400	Uncontrolled Resource Consumption	3,23	0	+13
25	CWE-306	Missing Authentication for Critical Function	2,73	5	-5

The top 20 vendors whose solutions were reported as vulnerable accounted for 29% of all newly disclosed documented vulnerabilities over the reporting period, with top three vendors with the highest count of vulnerabilities disclosed as high and critical being Microsoft, Adobe, and Qualcomm Inc.

Fig. 46 - Top 20 vendors across all disclosed vulnerabilities over the reporting period.
Source: EUVD



It should be noted that this distribution is likely to be inflated by CVE assignment policies, as is the case for Linux-related vulnerabilities, which also include bug fixes[482].

[482] http://www.kroah.com/log/blog/2024/02/13/linux-is-a-cna/

Based on CISA's catalogue of Known Exploited Vulnerabilities **(KEV)**[483]**, 245 vulnerabilities** were added over the reporting period, for which the top ten mentioned vendors concerned are displayed in Figure 47.

Fig. 47 - Most mentioned vendors in the KEV catalogue over the reporting period.
Source: CISA KEV

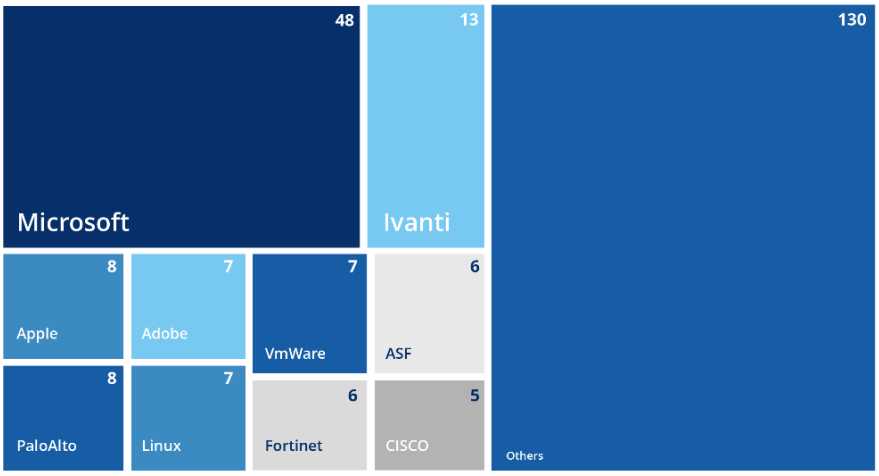
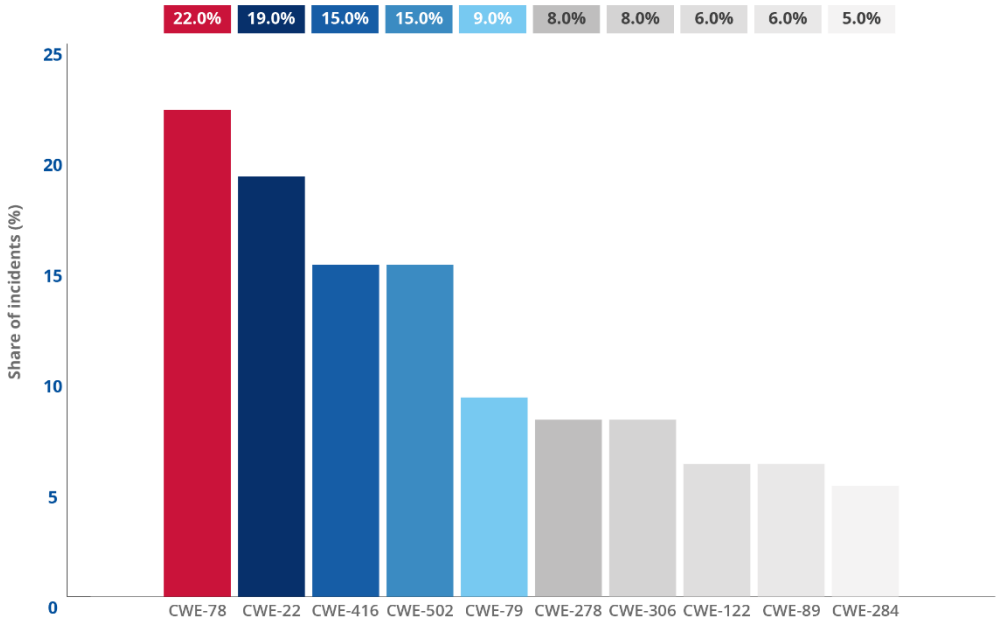


Fig. 48 - Top ten weaknesses leading to vulnerabilities added to the CISA KEV.
Source: US CISA KEV



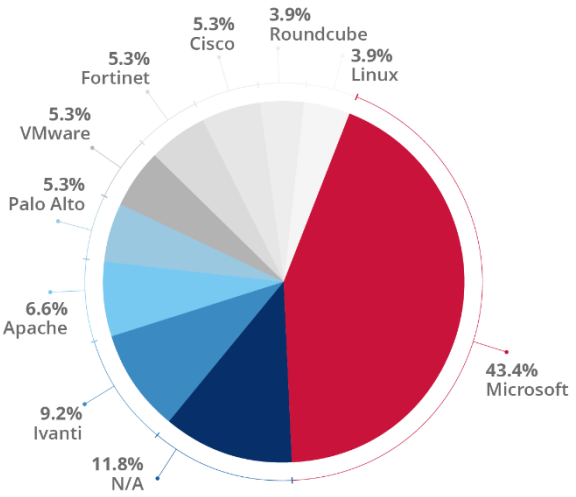
The top three Common Weakness Enumeration related to known exploited vulnerabilities in the reporting period are: CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), and CWE-416: Use After Free. All these weaknesses can cause vulnerabilities that allows in memory modification, code execution which could lead to take full control of the impacted system, as well crashes and denial of service, impacting the availability of the services run on or through the impacted system.

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

From an EU vantage point and based on ENISA's open-source collection, at least 115 exploited vulnerabilities were reported impacting and/or targeting EU MSs organisations[484].

This includes vulnerabilities that were subject to a coordinated publication of advisories by the European Union CSIRTs Network (CNW) members[485] [486] and confirmed to be exploited in open sources. While not the only factor, **vulnerability distribution also speaks to the equipment rate in the EU**. For instance, Microsoft largely dominates across the environments of consumers and public and private organisations[487].

Fig. 49 - Most mentioned vendors across vulnerabilities exploited in the EU.
Source: ENISA dataset



Further analysis of the ENISA dataset with vulnerabilities matched against MITRE ATT&CK IDs confirms that **attackers consistently exploit Internet-facing applications** (T1190). Vulnerabilities impacting Confluence, Exchange (ProxyLogon/ProxyShell), Citrix NetScaler, Fortinet/Check Point/Palo Alto VPN appliances, PaperCut, TeamCity, ActiveMQ, vCenter and Zimbra dominate the set — typical of mass-exploitation waves where perimeter services are scanned and compromised within hours of disclosure.

A smaller but critical part consists of local privilege-escalation (T1068) under which vulnerabilities such as PwnKit and Windows CLFS were exploited, which enable webshell footholds into SYSTEM/Domain Admin and facilitate lateral movement. On the end-user side, client execution (T1203) remains prevalent (Office Equation Editor, WinRAR, browser zero-days), almost always appearing alongside phishing (T1566.001) or drive-by compromise (T1189) as the delivery vector.

These TTPs reflect a **combination of opportunistic exploitation of exposed services and targeted post-exploitation** to maintain persistence, escalate privileges and exfiltrate data.

10.3 RECOMMENDATIONS

Based on identified TTPs, including the vulnerabilities listed hereabove, all identified malware types stress **execution prevention, endpoint behaviour monitoring, privilege control, network filtering, auditing and user training**, forming the baseline of cyber hygiene. Together, the three categories illustrate the need for an evolving defensive posture: from **preventing initial compromise,** to **containing impact,** to **safeguarding against long-term remote access.**

For loaders, mitigations focus heavily on **blocking initial execution** and **persistence**. Restricting registry, DLLs and software installation are central, reflecting loaders' role as initial footholds. Mitigation against ransomware build on the loader baseline but emphasise the **need for resilience and business continuity**. Backup, remote storage, data loss prevention and network segmentation are critical. Identity management (password policies, MFA implementation) is reinforced since ransomware operators rely on credential abuse during lateral spread. Sharing ransomware's depth mitigation measures against RAT also include controls against long-term persistence (library loading restrictions, account use policies). RAT mitigations reflect both stealthy footholds and

[484] See Appendix
[485] https://csirtsnetwork.eu/
[486] https://github.com/enisaeu/CNW/blob/main/advisories/README.md
[487] https://gs.statcounter.com/os-market-share/all/europe

extended command-and-control activity, blending loader-style entry controls with ransomware-style resilience measures.

10.4 SYSTEM HARDENING

Strengthening the foundation of operating environments is central for prevention. Measures include Execution Prevention (M1038) and Behaviour Prevention on Endpoint (M1040). Baseline controls such as Operating System Configuration (M1028), Software Configuration (M1054), Active Directory Configuration (M1015) reduce the attack surface. Additional safeguards include Restrict Registry Permissions (M1024), Restrict File and Directory Permissions (M1022), Restrict Library Loading (M1044). Validation mechanisms such as Code Signing (M1045), Disable or Remove Feature or Program (M1042) further reduce exposure by ensuring only trusted components and essential features are present.

10.5 ACCESS & PRIVILEGE

Identity and access controls form a critical line of defence. These include User Account Management (M1018), Privileged Account Management (M1026), User Account Control (M1052), which enforce least-privilege principles. Limit Software Installation (M1033) reduces unauthorised application deployment. To counter credential misuse, Password Policies (M1027) and Multi-Factor Authentication (M1032) strengthen identity assurance, while Account Use Policies (M1035) ensure proper oversight of account activity.

10.6 NETWORK PROTECTIONS

Preventing malicious communication and lateral spread relies on layered network defences. Network Intrusion Prevention (M1031) and Filter Network Traffic (M1037) provide frontline detection and blocking. Network Segmentation (M1030) contains threats within isolated zones, while Restrict Web-Based Content (M1021) reduces exposure to drive-by downloads and malicious sites. To further limit unauthorised communications, Limit Access to Resource Over Network (M1048) enforces strict control over resource availability across the network.

10.7 MONITORING

Effective oversight ensures early detection of malicious activity. Audit (M1047) provides system and activity logging, while Application Developer Guidance (M1013) reduces exploitable flaws through secure design. Complementary policies such as Account Use Policies (M1035) and Limit Access to Resource Over Network (M1048) enforce consistent monitoring of identity and network activity to detect anomalies.

10.8 RESILIENCE

Assuming that some attacks may succeed, resilience controls minimize impact and accelerate recovery. Data Backup (M1053) and Remote Data Storage (M1029) ensure continuity of operations. Data Loss Prevention (M1057) and Encrypt Sensitive Information (M1041) protect confidentiality and integrity even under compromise. Preventive measures such as Update Software (M1051) and Antivirus/Antimalware (M1049) reduce exploitable weaknesses, while User Training (M1017) equips staff to recognise and resist social engineering attempts.

11. OUTLOOK & CONCLUSION

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 cybercriminal ecosystem.

In terms of impact, the EU threat picture will remain dominated by opportunistic cybercriminal activities involving the use of ransomware and information-stealers, despite the achievements of law-enforcement. Displaced or disrupted RaaS brands will continue being promptly replaced by emerging programmes. The criminal marketplace will continue formalising around skills to further scale campaigns, notably through AI integration, IoT and large-scale exploitations of vulnerabilities and the targeting of critical sectors, notably hosting companies and IT providers. The rising use of EDR-kill tooling (e.g., AvNeutralizer, EDRKillShifter) and BYOVD, as well as legal-pressure features in extortion playbooks, will sharpen both the speed and leverage of intrusions. Hacktivist-led DDoS will persist as a nuisance, both in terms of the disruption of business continuity and in the information operation sphere, highly likely with spikes around high visibility events and announcements by EU MSs and EU entities and authorities. State-nexus intrusion sets will continue to blend espionage, supply-chain access and IO, increasingly leaning on compromised EU-hosted infrastructure.

Looking forward, cyber threat activity is likely to further intensify along three dimensions: convergence, automation and industrialisation. AI will accelerate cycles of offensive innovation, enabling rapid campaign development and more effective deception techniques. Abuse of cyber dependencies will remain a strategic priority, while the persistence of hacktivism and disinformation campaigns will continue to influence public perception and policy debates.

The highlights of this report underscore how defensive strategies must become intelligence-driven and systemic, emphasising proactive threat hunting, behavioural detection and the integration of cyber risk management into broader operational and policy frameworks. Organisations should prioritise comprehensive asset discovery, automated vulnerability management and resilience planning for interconnected systems and services. Collaboration between Member States, EU institutions and private industry is essential for countering the threats.

In parallel, the European policy landscape is evolving to address these challenges. The Cyber Resilience Act (CRA) introduces mandatory security requirements for digital products and services, aimed at reducing systemic vulnerabilities by embedding security-by-design practices and formalising vulnerability disclosure obligations. The Cyber Solidarity Act (CSoA) strengthens Europe’s collective defence by improving mechanisms for cross-border incident response and the coordinated sharing of threat intelligence. The updated Cybersecurity Blueprint further supports these efforts by creating structured escalation paths and standardised response procedures for large-scale incidents. Together, these frameworks provide the foundation for a more unified and proactive cybersecurity posture across the EU.

In close cooperation with Union entities, ENISA is central to translating these policy measures into tangible outcomes. Its work on situational awareness, operational cooperation, support for critical sectors, certification schemes, capacity building and policy monitoring ensures that regulatory initiatives are supported by strategic and operational expertise. Through coordination of the CSIRT Network, support to CyCLONe, and the development of taxonomies and reporting frameworks, ENISA helps to harmonise reporting obligations and improve the visibility of systemic risks. Annual threat assessments, red-teaming exercises and sector-specific guidance further reinforce the EU’s readiness, enabling organisations and Member States to operationalise regulatory requirements.

12. APPENDIX

12.1 TACTICS, TECHNIQUES & PROCEDURES (TTPS)

MITRE ATT&CK Enterprise TTPs identified for loaders reportedly seen in the EU

Tactic	Technique	Mitigation
TA0009: Collection	T1005: Data from Local System	M1057: Data Loss Prevention
TA0007: Discovery	T1007: System Service Discovery	
TA0007: Discovery	T1012: Query Registry	
TA0007: Discovery	T1016: System Network Configuration Discovery	
TA-OTHER: Other	T1027: Obfuscated Files or Information	M1047: Audit, M1040: Behaviour Prevention on Endpoint, M1017: User Training, M1049: Antivirus/Antimalware
TA-OTHER: Other	T1055: Process Injection	M1026: Privileged Account Management, M1040: Behaviour Prevention on Endpoint
TA-OTHER: Other	T1055.003: Thread Execution Hijacking	M1040: Behaviour Prevention on Endpoint, M1026: Privileged Account Management
TA0007: Discovery	T1057: Process Discovery	
TA-OTHER: Other	T1070.004: File Deletion	M1041: Encrypt Sensitive Information, M1029: Remote Data Storage, M1022: Restrict File and Directory Permissions
TA-OTHER: Other	T1071.001: Web Protocols	M1031: Network Intrusion Prevention, M1037: Filter Network Traffic
TA0007: Discovery	T1082: System Information Discovery	
TA0007: Discovery	T1083: File and Directory Discovery	
TA-OTHER: Other	T1105: Ingress Tool Transfer	M1031: Network Intrusion Prevention
TA0003: Persistence	T1112: Modify Registry	M1024: Restrict Registry Permissions
TA-OTHER: Other	T1134: Access Token Manipulation	M1018: User Account Management, M1026: Privileged Account Management
TA0007: Discovery	T1135: Network Share Discovery	M1028: Operating System Configuration
TA0002: Execution	T1204.002: Malicious File	M1038: Execution Prevention, M1040: Behaviour Prevention on Endpoint, M1017: User Training, M1021: Restrict Web-Based Content, M1031: Network Intrusion Prevention
TA0003: Persistence	T1543.003: Windows Service	M1040: Behaviour Prevention on Endpoint, M1028: Operating System Configuration, M1047: Audit, M1045: Code Signing, M1018: User Account Management, M1033: Limit Software Installation, M1026: Privileged Account Management, M1054: Software Configuration, M1022: Restrict File and Directory Permissions

Tactic	Technique	Mitigation
TA0003: Persistence	T1546.015: Component Object Model Hijacking	M1026: Privileged Account Management, M1051: Update Software
TA-OTHER: Other	T1566.001: Spearphishing Attachment	M1049: Antivirus/Antimalware, M1018: User Account Management, M1047: Audit, M1031: Network Intrusion Prevention, M1054: Software Configuration, M1017: User Training, M1021: Restrict Web-Based Content
TA-OTHER: Other	T1572: Protocol Tunnelling	M1037: Filter Network Traffic, M1031: Network Intrusion Prevention
TA0003: Persistence	T1574.001: DLL	M1038: Execution Prevention, M1044: Restrict Library Loading, M1051: Update Software, M1047: Audit, M1013: Application Developer Guidance, M1052: User Account Control, M1040: Behaviour Prevention on Endpoint, M1018: User Account Management, M1022: Restrict File and Directory Permissions, M1024: Restrict Registry Permissions
TA0003: Persistence	T1574.002: DLL Side-Loading	M1052: User Account Control, M1040: Behaviour Prevention on Endpoint, M1044: Restrict Library Loading, M1047: Audit, M1013: Application Developer Guidance, M1018: User Account Management, M1051: Update Software, M1038: Execution Prevention, M1022: Restrict File and Directory Permissions, M1024: Restrict Registry Permissions

MITRE ATT&CK Enterprise TTPs identified for RATs reportedly seen in the EU

Tactic	Technique	Mitigation
TA-OTHER: Other	T1001.001: Junk Data	M1031: Network Intrusion Prevention
TA-OTHER: Other	T1003: OS Credential Dumping	M1041: Encrypt Sensitive Information, M1040: Behaviour Prevention on Endpoint, M1027: Password Policies, M1017: User Training, M1026: Privileged Account Management, M1025: Privileged Process Integrity, M1043: Credential Access Protection, M1015: Active Directory Configuration, M1028: Operating System Configuration
TA-OTHER: Other	T1003.001: LSASS Memory	M1028: Operating System Configuration, M1043: Credential Access Protection, M1025: Privileged Process Integrity, M1026: Privileged Account Management, M1017: User Training, M1040: Behaviour Prevention on Endpoint, M1027: Password Policies, M1041: Encrypt Sensitive Information, M1015: Active Directory Configuration
TA-OTHER: Other	T1003.003: NTDS	M1027: Password Policies, M1026: Privileged Account Management, M1017: User Training, M1041: Encrypt Sensitive Information, M1040: Behaviour Prevention on Endpoint, M1025: Privileged Process Integrity, M1043: Credential Access Protection, M1015:

Tactic	Technique	Mitigation
		Active Directory Configuration, M1028: Operating System Configuration
TA0009: Collection	T1005: Data from Local System	M1057: Data Loss Prevention
TA0007: Discovery	T1007: System Service Discovery	
TA0007: Discovery	T1010: Application Window Discovery	
TA0010: Exfiltration	T1011.001: Exfiltration Over Bluetooth	M1042: Disable or Remove Feature or Program, M1028: Operating System Configuration
TA-OTHER: Other	T1014: Rootkit	
TA0007: Discovery	T1016: System Network Configuration Discovery	
TA0007: Discovery	T1018: Remote System Discovery	
TA-OTHER: Other	T1021.001: Remote Desktop Protocol	M1047: Audit, M1035: Limit Access to Resource Over Network, M1030: Network Segmentation, M1028: Operating System Configuration, M1042: Disable or Remove Feature or Program, M1018: User Account Management, M1032: Multi-factor Authentication, M1026: Privileged Account Management, M1027: Password Policies
TA-OTHER: Other	T1021.004: SSH	M1042: Disable or Remove Feature or Program, M1032: Multi-factor Authentication, M1018: User Account Management, M1035: Limit Access to Resource Over Network, M1047: Audit, M1027: Password Policies
TA-OTHER: Other	T1027: Obfuscated Files or Information	M1047: Audit, M1040: Behaviour Prevention on Endpoint, M1017: User Training, M1049: Antivirus/Antimalware
TA-OTHER: Other	T1027.001: Binary Padding	M1047: Audit, M1040: Behaviour Prevention on Endpoint, M1017: User Training, M1049: Antivirus/Antimalware
TA-OTHER: Other	T1027.002: Software Packing	M1049: Antivirus/Antimalware, M1047: Audit, M1040: Behaviour Prevention on Endpoint, M1017: User Training
TA0007: Discovery	T1033: System Owner/User Discovery	
TA-OTHER: Other	T1036: Masquerading	M1047: Audit, M1018: User Account Management, M1017: User Training, M1045: Code Signing, M1040: Behaviour Prevention on Endpoint, M1022: Restrict File and Directory Permissions, M1049: Antivirus/Antimalware, M1038: Execution Prevention
TA-OTHER: Other	T1036.004: Masquerade Task or Service	M1047: Audit, M1018: User Account Management, M1017: User Training, M1045: Code Signing, M1040: Behaviour Prevention on Endpoint, M1022: Restrict File and Directory Permissions, M1049: Antivirus/Antimalware, M1038: Execution Prevention

Tactic	Technique	Mitigation
TA-OTHER: Other	T1036.005: Match Legitimate Resource Name or Location	M1022: Restrict File and Directory Permissions, M1038: Execution Prevention, M1045: Code Signing, M1047: Audit, M1018: User Account Management, M1017: User Training, M1040: Behaviour Prevention on Endpoint, M1049: Antivirus/Antimalware
TA0003: Persistence	T1037: Boot or Logon Initialisation Scripts	M1024: Restrict Registry Permissions, M1022: Restrict File and Directory Permissions
TA0010: Exfiltration	T1041: Exfiltration Over C2 Channel	M1031: Network Intrusion Prevention, M1057: Data Loss Prevention
TA0007: Discovery	T1046: Network Service Discovery	M1042: Disable or Remove Feature or Program, M1031: Network Intrusion Prevention, M1030: Network Segmentation
TA0002: Execution	T1047: Windows Management Instrumentation	M1026: Privileged Account Management, M1040: Behaviour Prevention on Endpoint, M1018: User Account Management, M1038: Execution Prevention
TA0010: Exfiltration	T1048: Exfiltration Over Alternative Protocol	M1030: Network Segmentation, M1057: Data Loss Prevention, M1037: Filter Network Traffic, M1031: Network Intrusion Prevention, M1022: Restrict File and Directory Permissions, M1018: User Account Management
TA0010: Exfiltration	T1052.001: Exfiltration over USB	M1042: Disable or Remove Feature or Program, M1034: Limit Hardware Installation, M1057: Data Loss Prevention
TA0002: Execution	T1053: Scheduled Task/Job	M1018: User Account Management, M1028: Operating System Configuration, M1022: Restrict File and Directory Permissions, M1026: Privileged Account Management, M1047: Audit
TA0003: Persistence	T1053: Scheduled Task/Job	M1018: User Account Management, M1028: Operating System Configuration, M1022: Restrict File and Directory Permissions, M1026: Privileged Account Management, M1047: Audit
TA0002: Execution	T1053.005: Scheduled Task	M1026: Privileged Account Management, M1018: User Account Management, M1047: Audit, M1028: Operating System Configuration, M1022: Restrict File and Directory Permissions
TA0003: Persistence	T1053.005: Scheduled Task	M1026: Privileged Account Management, M1018: User Account Management, M1047: Audit, M1028: Operating System Configuration, M1022: Restrict File and Directory Permissions
TA-OTHER: Other	T1055: Process Injection	M1026: Privileged Account Management, M1040: Behaviour Prevention on Endpoint
TA-OTHER: Other	T1055.002: Portable Executable Injection	M1040: Behaviour Prevention on Endpoint, M1026: Privileged Account Management

Tactic	Technique	Mitigation
TA0009: Collection	T1056: Input Capture	
TA0007: Discovery	T1057: Process Discovery	
TA0002: Execution	T1059: Command and Scripting Interpreter	M1033: Limit Software Installation, M1045: Code Signing, M1042: Disable or Remove Feature or Program, M1038: Execution Prevention, M1049: Antivirus/Antimalware, M1026: Privileged Account Management, M1047: Audit, M1021: Restrict Web-Based Content, M1040: Behaviour Prevention on Endpoint
TA0002: Execution	T1059.001: PowerShell	M1042: Disable or Remove Feature or Program, M1049: Antivirus/Antimalware, M1045: Code Signing, M1026: Privileged Account Management, M1038: Execution Prevention, M1033: Limit Software Installation, M1047: Audit, M1021: Restrict Web-Based Content, M1040: Behaviour Prevention on Endpoint
TA0002: Execution	T1059.003: Windows Command Shell	M1038: Execution Prevention, M1033: Limit Software Installation, M1045: Code Signing, M1042: Disable or Remove Feature or Program, M1049: Antivirus/Antimalware, M1026: Privileged Account Management, M1047: Audit, M1021: Restrict Web-Based Content, M1040: Behaviour Prevention on Endpoint
TA0002: Execution	T1059.005: Visual Basic	M1042: Disable or Remove Feature or Program, M1049: Antivirus/Antimalware, M1038: Execution Prevention, M1040: Behaviour Prevention on Endpoint, M1021: Restrict Web-Based Content, M1033: Limit Software Installation, M1045: Code Signing, M1026: Privileged Account Management, M1047: Audit
TA-OTHER: Other	T1068: Exploitation for Privilege Escalation	M1051: Update Software, M1050: Exploit Protection, M1048: Application Isolation and Sandboxing, M1019: Threat Intelligence Program, M1038: Execution Prevention
TA0007: Discovery	T1069.001: Local Groups	
TA0007: Discovery	T1069.002: Domain Groups	
TA-OTHER: Other	T1070.001: Clear Windows Event Logs	M1022: Restrict File and Directory Permissions, M1029: Remote Data Storage, M1041: Encrypt Sensitive Information
TA-OTHER: Other	T1070.004: File Deletion	M1041: Encrypt Sensitive Information, M1029: Remote Data Storage, M1022: Restrict File and Directory Permissions
TA-OTHER: Other	T1071: Application Layer Protocol	M1031: Network Intrusion Prevention, M1037: Filter Network Traffic
TA-OTHER: Other	T1071.001: Web Protocols	M1031: Network Intrusion Prevention, M1037: Filter Network Traffic
TA0009: Collection	T1074: Data Staged	

Tactic	Technique	Mitigation
TA0003: Persistence	T1078: Valid Accounts	M1027: Password Policies, M1018: User Account Management, M1026: Privileged Account Management, M1032: Multi-factor Authentication, M1013: Application Developer Guidance, M1017: User Training, M1015: Active Directory Configuration, M1036: Account Use Policies
TA-OTHER: Other	T1080: Taint Shared Content	M1049: Antivirus/Antimalware, M1038: Execution Prevention, M1022: Restrict File and Directory Permissions, M1050: Exploit Protection
TA0007: Discovery	T1082: System Information Discovery	
TA0007: Discovery	T1083: File and Directory Discovery	
TA0007: Discovery	T1087.002: Domain Account	M1028: Operating System Configuration, M1018: User Account Management
TA-OTHER: Other	T1105: Ingress Tool Transfer	M1031: Network Intrusion Prevention
TA0002: Execution	T1106: Native API	M1038: Execution Prevention, M1040: Behaviour Prevention on Endpoint
TA-OTHER: Other	T1110: Brute Force	M1018: User Account Management, M1036: Account Use Policies, M1032: Multi-factor Authentication, M1027: Password Policies
TA0003: Persistence	T1112: Modify Registry	M1024: Restrict Registry Permissions
TA0002: Execution	T1129: Shared Modules	M1038: Execution Prevention
TA0003: Persistence	T1133: External Remote Services	M1030: Network Segmentation, M1042: Disable or Remove Feature or Program, M1035: Limit Access to Resource Over Network, M1032: Multi-factor Authentication
TA-OTHER: Other	T1134: Access Token Manipulation	M1018: User Account Management, M1026: Privileged Account Management
TA0007: Discovery	T1135: Network Share Discovery	M1028: Operating System Configuration
TA-OTHER: Other	T1140: Deobfuscate/Decode Files or Information	
TA-OTHER: Other	T1190: Exploit Public-Facing Application	M1048: Application Isolation and Sandboxing, M1030: Network Segmentation, M1016: Vulnerability Scanning, M1026: Privileged Account Management, M1050: Exploit Protection, M1035: Limit Access to Resource Over Network, M1051: Update Software
TA-OTHER: Other	T1202: Indirect Command Execution	
TA0002: Execution	T1204: User Execution	M1017: User Training, M1038: Execution Prevention, M1040: Behaviour Prevention on Endpoint, M1021: Restrict Web-Based Content, M1031: Network Intrusion Prevention
TA0002: Execution	T1204.001: Malicious Link	M1031: Network Intrusion Prevention, M1017: User Training, M1021: Restrict Web-Based Content, M1038: Execution

Tactic	Technique	Mitigation
		Prevention, M1040: Behaviour Prevention on Endpoint
TA0002: Execution	T1204.002: Malicious File	M1038: Execution Prevention, M1040: Behaviour Prevention on Endpoint, M1017: User Training, M1021: Restrict Web-Based Content, M1031: Network Intrusion Prevention
TA-OTHER: Other	T1211: Exploitation for Defence Evasion	M1050: Exploit Protection, M1051: Update Software, M1019: Threat Intelligence Program, M1048: Application Isolation and Sandboxing
TA0009: Collection	T1213.002: SharePoint	M1047: Audit, M1018: User Account Management, M1017: User Training, M1032: Multi-factor Authentication, M1060: Out-of-Band Communications Channel, M1054: Software Configuration, M1041: Encrypt Sensitive Information
TA-OTHER: Other	T1218.007: Msiexec	M1042: Disable or Remove Feature or Program, M1026: Privileged Account Management, M1050: Exploit Protection, M1037: Filter Network Traffic, M1038: Execution Prevention, M1021: Restrict Web-Based Content
TA-OTHER: Other	T1219: Remote Access Tools	M1038: Execution Prevention, M1037: Filter Network Traffic, M1034: Limit Hardware Installation, M1031: Network Intrusion Prevention, M1042: Disable or Remove Feature or Program
TA-OTHER: Other	T1222: File and Directory Permissions Modification	M1022: Restrict File and Directory Permissions, M1026: Privileged Account Management
TA-OTHER: Other	T1222.001: Windows File and Directory Permissions Modification	M1026: Privileged Account Management, M1022: Restrict File and Directory Permissions
TA-OTHER: Other	T1222.002: Linux and Mac File and Directory Permissions Modification	M1022: Restrict File and Directory Permissions, M1026: Privileged Account Management
TA-OTHER: Other	T1407	
TA-OTHER: Other	T1409	
TA-OTHER: Other	T1417.001	
TA-OTHER: Other	T1417.002	
TA-OTHER: Other	T1418	
TA-OTHER: Other	T1424	
TA-OTHER: Other	T1426	
TA-OTHER: Other	T1429	
TA-OTHER: Other	T1456	
TA-OTHER: Other	T1471	
TA-OTHER: Other	T1480: Execution Guardrails	M1055: Do Not Mitigate

Tactic	Technique	Mitigation
TA-OTHER: Other	T1480.002: Mutual Exclusion	M1055: Do Not Mitigate
TA0007: Discovery	T1482: Domain Trust Discovery	M1047: Audit, M1030: Network Segmentation
TA-OTHER: Other	T1484.001: Group Policy Modification	M1047: Audit, M1018: User Account Management, M1026: Privileged Account Management
TA0040: Impact	T1485: Data Destruction	M1032: Multi-factor Authentication, M1053: Data Backup, M1018: User Account Management
TA0040: Impact	T1486: Data Encrypted for Impact	M1040: Behaviour Prevention on Endpoint, M1053: Data Backup
TA0040: Impact	T1489: Service Stop	M1030: Network Segmentation, M1018: User Account Management, M1060: Out-of-Band Communications Channel, M1024: Restrict Registry Permissions, M1022: Restrict File and Directory Permissions
TA0040: Impact	T1490: Inhibit System Recovery	M1038: Execution Prevention, M1028: Operating System Configuration, M1018: User Account Management, M1053: Data Backup
TA0040: Impact	T1491.001: Internal Defacement	M1053: Data Backup
TA0007: Discovery	T1497: Virtualisation/Sandbox Evasion	
TA0007: Discovery	T1497.001: System Checks	
TA0007: Discovery	T1497.003: Time Based Evasion	
TA0007: Discovery	T1497.004: Virtualisation/Sandbox Evasion	
TA-OTHER: Other	T1513	
TA0007: Discovery	T1518.001: Security Software Discovery	
TA0040: Impact	T1529: System Shutdown/Reboot	
TA0040: Impact	T1531: Account Access Removal	
TA-OTHER: Other	T1533	
TA0003: Persistence	T1543.003: Windows Service	M1040: Behaviour Prevention on Endpoint, M1028: Operating System Configuration, M1047: Audit, M1045: Code Signing, M1018: User Account Management, M1033: Limit Software Installation, M1026: Privileged Account Management, M1054: Software Configuration, M1022: Restrict File and Directory Permissions
TA0003: Persistence	T1547: Boot or Logon Autostart Execution	
TA0003: Persistence	T1547.001: Registry Run Keys / Startup Folder	
TA-OTHER: Other	T1548: Abuse Elevation Control Mechanism	M1038: Execution Prevention, M1028: Operating System Configuration, M1051: Update Software, M1052: User Account

Tactic	Technique	Mitigation
		Control, M1026: Privileged Account Management, M1018: User Account Management, M1047: Audit, M1022: Restrict File and Directory Permissions
TA-OTHER: Other	T1548.002: Bypass User Account Control	M1051: Update Software, M1047: Audit, M1052: User Account Control, M1026: Privileged Account Management, M1038: Execution Prevention, M1028: Operating System Configuration, M1018: User Account Management, M1022: Restrict File and Directory Permissions
TA-OTHER: Other	T1552: Unsecured Credentials	M1041: Encrypt Sensitive Information, M1051: Update Software, M1017: User Training, M1015: Active Directory Configuration, M1027: Password Policies, M1028: Operating System Configuration, M1037: Filter Network Traffic, M1022: Restrict File and Directory Permissions, M1035: Limit Access to Resource Over Network, M1047: Audit, M1026: Privileged Account Management
TA-OTHER: Other	T1553.002: Code Signing	M1038: Execution Prevention, M1028: Operating System Configuration, M1026: Privileged Account Management, M1024: Restrict Registry Permissions, M1054: Software Configuration
TA-OTHER: Other	T1558: Steal or Forge Kerberos Tickets	M1015: Active Directory Configuration, M1043: Credential Access Protection, M1041: Encrypt Sensitive Information, M1027: Password Policies, M1047: Audit, M1026: Privileged Account Management
TA0009: Collection	T1560: Archive Collected Data	M1047: Audit
TA0009: Collection	T1560.001: Archive via Utility	M1047: Audit
TA0040: Impact	T1561.001: Disk Content Wipe	M1053: Data Backup
TA-OTHER: Other	T1562: Impair Defences	M1054: Software Configuration, M1018: User Account Management, M1038: Execution Prevention, M1022: Restrict File and Directory Permissions, M1024: Restrict Registry Permissions, M1047: Audit, M1042: Disable or Remove Feature or Program
TA-OTHER: Other	T1562.001: Disable or Modify Tools	M1038: Execution Prevention, M1024: Restrict Registry Permissions, M1018: User Account Management, M1022: Restrict File and Directory Permissions, M1047: Audit, M1054: Software Configuration, M1042: Disable or Remove Feature or Program
TA-OTHER: Other	T1562.004: Disable or Modify System Firewall	M1047: Audit, M1018: User Account Management, M1024: Restrict Registry Permissions, M1022: Restrict File and Directory Permissions, M1054: Software Configuration, M1038: Execution Prevention, M1042: Disable or Remove Feature or Program
TA-OTHER: Other	T1562.009: Safe Mode Boot	M1026: Privileged Account Management, M1054: Software Configuration, M1018: User Account

Tactic	Technique	Mitigation
		Management, M1038: Execution Prevention, M1022: Restrict File and Directory Permissions, M1024: Restrict Registry Permissions, M1047: Audit, M1042: Disable or Remove Feature or Program
TA-OTHER: Other	T1564: Hide Artifacts	M1033: Limit Software Installation, M1013: Application Developer Guidance, M1047: Audit, M1049: Antivirus/Antimalware
TA-OTHER: Other	T1564.001: Hidden Files and Directories	M1033: Limit Software Installation, M1013: Application Developer Guidance, M1047: Audit, M1049: Antivirus/Antimalware
TA-OTHER: Other	T1564.003: Hidden Window	M1038: Execution Prevention, M1033: Limit Software Installation, M1013: Application Developer Guidance, M1047: Audit, M1049: Antivirus/Antimalware
TA-OTHER: Other	T1566: Phishing	M1047: Audit, M1031: Network Intrusion Prevention, M1054: Software Configuration, M1021: Restrict Web-Based Content, M1049: Antivirus/Antimalware, M1017: User Training
TA-OTHER: Other	T1566.001: Spearphishing Attachment	M1049: Antivirus/Antimalware, M1018: User Account Management, M1047: Audit, M1031: Network Intrusion Prevention, M1054: Software Configuration, M1017: User Training, M1021: Restrict Web-Based Content
TA-OTHER: Other	T1566.002: Spearphishing Link	M1054: Software Configuration, M1021: Restrict Web-Based Content, M1047: Audit, M1018: User Account Management, M1017: User Training, M1031: Network Intrusion Prevention, M1049: Antivirus/Antimalware
TA0010: Exfiltration	T1567.002: Exfiltration to Cloud Storage	M1021: Restrict Web-Based Content, M1057: Data Loss Prevention
TA0002: Execution	T1569.002: Service Execution	M1026: Privileged Account Management, M1040: Behaviour Prevention on Endpoint, M1022: Restrict File and Directory Permissions, M1018: User Account Management
TA-OTHER: Other	T1570: Lateral Tool Transfer	M1037: Filter Network Traffic, M1031: Network Intrusion Prevention
TA0003: Persistence	T1574.002: DLL Side-Loading	M1052: User Account Control, M1040: Behaviour Prevention on Endpoint, M1044: Restrict Library Loading, M1047: Audit, M1013: Application Developer Guidance, M1018: User Account Management, M1051: Update Software, M1038: Execution Prevention, M1022: Restrict File and Directory Permissions, M1024: Restrict Registry Permissions
TA-OTHER: Other	T1582	
TA-OTHER: Other	T1583: Acquire Infrastructure	M1056: Pre-compromise
TA-OTHER: Other	T1587: Develop Capabilities	M1056: Pre-compromise

Tactic	Technique	Mitigation
TA0043: Reconnaissance	T1595: Active Scanning	M1056: Pre-compromise
TA0043: Reconnaissance	T1598: Phishing for Information	M1017: User Training, M1054: Software Configuration
TA0007: Discovery	T1614.001: System Language Discovery	
TA0007: Discovery	T1622: Debugger Evasion	
TA-OTHER: Other	T1629.001	
TA-OTHER: Other	T1636.003	
TA-OTHER: Other	T1644	
TA0040: Impact	T1657: Financial Theft	M1017: User Training, M1018: User Account Management
TA-OTHER: Other	T1660	

MITRE ATT&CK Enterprise TTPs identified for ransomware reportedly seen in the EU

Tactic	Technique	Mitigation
TA-OTHER: Other	T1003: OS Credential Dumping	M1041: Encrypt Sensitive Information, M1040: Behaviour Prevention on Endpoint, M1027: Password Policies, M1017: User Training, M1026: Privileged Account Management, M1025: Privileged Process Integrity, M1043: Credential Access Protection, M1015: Active Directory Configuration, M1028: Operating System Configuration
TA-OTHER: Other	T1003.001: LSASS Memory	M1028: Operating System Configuration, M1043: Credential Access Protection, M1025: Privileged Process Integrity, M1026: Privileged Account Management, M1017: User Training, M1040: Behaviour Prevention on Endpoint, M1027: Password Policies, M1041: Encrypt Sensitive Information, M1015: Active Directory Configuration
TA0007: Discovery	T1016: System Network Configuration Discovery	
TA0007: Discovery	T1018: Remote System Discovery	
TA-OTHER: Other	T1021.001: Remote Desktop Protocol	M1047: Audit, M1035: Limit Access to Resource Over Network, M1030: Network Segmentation, M1028: Operating System Configuration, M1042: Disable or Remove Feature or Program, M1018: User Account Management, M1032: Multi-factor Authentication, M1026: Privileged Account Management, M1027: Password Policies
TA-OTHER: Other	T1021.002: SMB/Windows Admin Shares	M1026: Privileged Account Management, M1035: Limit Access to Resource Over Network, M1037: Filter Network Traffic, M1027: Password Policies, M1047: Audit, M1018: User Account Management, M1042: Disable

Tactic	Technique	Mitigation
		or Remove Feature or Program, M1032: Multi-factor Authentication
TA-OTHER: Other	T1027: Obfuscated Files or Information	M1047: Audit, M1040: Behaviour Prevention on Endpoint, M1017: User Training, M1049: Antivirus/Antimalware
TA-OTHER: Other	T1027.002: Software Packing	M1049: Antivirus/Antimalware, M1047: Audit, M1040: Behaviour Prevention on Endpoint, M1017: User Training
TA-OTHER: Other	T1027.013: Encrypted/Encoded File	M1049: Antivirus/Antimalware, M1040: Behaviour Prevention on Endpoint, M1047: Audit, M1017: User Training
TA-OTHER: Other	T1036.005: Match Legitimate Resource Name or Location	M1022: Restrict File and Directory Permissions, M1038: Execution Prevention, M1045: Code Signing, M1047: Audit, M1018: User Account Management, M1017: User Training, M1040: Behaviour Prevention on Endpoint, M1049: Antivirus/Antimalware
TA0003: Persistence	T1037: Boot or Logon Initialisation Scripts	M1024: Restrict Registry Permissions, M1022: Restrict File and Directory Permissions
TA0010: Exfiltration	T1041: Exfiltration Over C2 Channel	M1031: Network Intrusion Prevention, M1057: Data Loss Prevention
TA0007: Discovery	T1046: Network Service Discovery	M1042: Disable or Remove Feature or Program, M1031: Network Intrusion Prevention, M1030: Network Segmentation
TA0002: Execution	T1047: Windows Management Instrumentation	M1026: Privileged Account Management, M1040: Behaviour Prevention on Endpoint, M1018: User Account Management, M1038: Execution Prevention
TA0010: Exfiltration	T1048.002: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	M1031: Network Intrusion Prevention, M1030: Network Segmentation, M1037: Filter Network Traffic, M1057: Data Loss Prevention, M1022: Restrict File and Directory Permissions, M1018: User Account Management
TA0010: Exfiltration	T1048.003: Exfiltration Over Unencrypted Non-C2 Protocol	M1031: Network Intrusion Prevention, M1057: Data Loss Prevention, M1037: Filter Network Traffic, M1030: Network Segmentation, M1022: Restrict File and Directory Permissions, M1018: User Account Management
TA-OTHER: Other	T1055: Process Injection	M1026: Privileged Account Management, M1040: Behaviour Prevention on Endpoint
TA0009: Collection	T1056: Input Capture	
TA0007: Discovery	T1057: Process Discovery	
TA0002: Execution	T1059: Command and Scripting Interpreter	M1033: Limit Software Installation, M1045: Code Signing, M1042: Disable or Remove Feature or Program, M1038: Execution Prevention, M1049: Antivirus/Antimalware, M1026: Privileged Account Management, M1047: Audit, M1021: Restrict Web-Based Content,

Tactic	Technique	Mitigation
		M1040: Behaviour Prevention on Endpoint
TA0002: Execution	T1059.001: PowerShell	M1042: Disable or Remove Feature or Program, M1049: Antivirus/Antimalware, M1045: Code Signing, M1026: Privileged Account Management, M1038: Execution Prevention, M1033: Limit Software Installation, M1047: Audit, M1021: Restrict Web-Based Content, M1040: Behaviour Prevention on Endpoint
TA0002: Execution	T1059.003: Windows Command Shell	M1038: Execution Prevention, M1033: Limit Software Installation, M1045: Code Signing, M1042: Disable or Remove Feature or Program, M1049: Antivirus/Antimalware, M1026: Privileged Account Management, M1047: Audit, M1021: Restrict Web-Based Content, M1040: Behaviour Prevention on Endpoint
TA0002: Execution	T1059.005: Visual Basic	M1042: Disable or Remove Feature or Program, M1049: Antivirus/Antimalware, M1038: Execution Prevention, M1040: Behaviour Prevention on Endpoint, M1021: Restrict Web-Based Content, M1033: Limit Software Installation, M1045: Code Signing, M1026: Privileged Account Management, M1047: Audit
TA-OTHER: Other	T1070.001: Clear Windows Event Logs	M1022: Restrict File and Directory Permissions, M1029: Remote Data Storage, M1041: Encrypt Sensitive Information
TA-OTHER: Other	T1070.004: File Deletion	M1041: Encrypt Sensitive Information, M1029: Remote Data Storage, M1022: Restrict File and Directory Permissions
TA-OTHER: Other	T1071.001: Web Protocols	M1031: Network Intrusion Prevention, M1037: Filter Network Traffic
TA-OTHER: Other	T1071.002: File Transfer Protocols	M1031: Network Intrusion Prevention, M1037: Filter Network Traffic
TA0002: Execution	T1072: Software Deployment Tools	M1018: User Account Management, M1015: Active Directory Configuration, M1051: Update Software, M1026: Privileged Account Management, M1027: Password Policies, M1033: Limit Software Installation, M1030: Network Segmentation, M1017: User Training, M1032: Multi-factor Authentication, M1029: Remote Data Storage
TA0003: Persistence	T1078: Valid Accounts	M1027: Password Policies, M1018: User Account Management, M1026: Privileged Account Management, M1032: Multi-factor Authentication, M1013: Application Developer Guidance, M1017: User Training, M1015: Active Directory Configuration, M1036: Account Use Policies
TA0003: Persistence	T1078.002: Domain Accounts	M1018: User Account Management, M1032: Multi-factor Authentication, M1026: Privileged Account Management, M1017: User Training, M1027: Password Policies, M1013:

Tactic	Technique	Mitigation
		Application Developer Guidance, M1015: Active Directory Configuration, M1036: Account Use Policies
TA0003: Persistence	T1078.003: Local Accounts	M1026: Privileged Account Management, M1032: Multi-factor Authentication, M1027: Password Policies, M1018: User Account Management, M1013: Application Developer Guidance, M1017: User Training, M1015: Active Directory Configuration, M1036: Account Use Policies
TA0007: Discovery	T1082: System Information Discovery	
TA0007: Discovery	T1083: File and Directory Discovery	
TA-OTHER: Other	T1095: Non-Application Layer Protocol	M1031: Network Intrusion Prevention, M1047: Audit, M1037: Filter Network Traffic, M1030: Network Segmentation
TA-OTHER: Other	T1102: Web Service	M1031: Network Intrusion Prevention, M1021: Restrict Web-Based Content
TA-OTHER: Other	T1105: Ingress Tool Transfer	M1031: Network Intrusion Prevention
TA0002: Execution	T1106: Native API	M1038: Execution Prevention, M1040: Behaviour Prevention on Endpoint
TA-OTHER: Other	T1110: Brute Force	M1018: User Account Management, M1036: Account Use Policies, M1032: Multi-factor Authentication, M1027: Password Policies
TA0003: Persistence	T1112: Modify Registry	M1024: Restrict Registry Permissions
TA0009: Collection	T1119: Automated Collection	M1029: Remote Data Storage, M1041: Encrypt Sensitive Information
TA0007: Discovery	T1120: Peripheral Device Discovery	
TA0007: Discovery	T1124: System Time Discovery	
TA-OTHER: Other	T1132.001: Standard Encoding	M1031: Network Intrusion Prevention
TA0003: Persistence	T1133: External Remote Services	M1030: Network Segmentation, M1042: Disable or Remove Feature or Program, M1035: Limit Access to Resource Over Network, M1032: Multi-factor Authentication
TA0007: Discovery	T1135: Network Share Discovery	M1028: Operating System Configuration
TA0003: Persistence	T1136: Create Account	M1030: Network Segmentation, M1028: Operating System Configuration, M1032: Multi-factor Authentication, M1026: Privileged Account Management
TA-OTHER: Other	T1140: Deobfuscate/Decode Files or Information	
TA-OTHER: Other	T1189: Drive-by Compromise	M1050: Exploit Protection, M1051: Update Software, M1048: Application Isolation and Sandboxing, M1021: Restrict Web-Based Content, M1017: User Training

Tactic	Technique	Mitigation
TA-OTHER: Other	T1190: Exploit Public-Facing Application	M1048: Application Isolation and Sandboxing, M1030: Network Segmentation, M1016: Vulnerability Scanning, M1026: Privileged Account Management, M1050: Exploit Protection, M1035: Limit Access to Resource Over Network, M1051: Update Software
TA-OTHER: Other	T1218.003: CMSTP	M1038: Execution Prevention, M1042: Disable or Remove Feature or Program, M1050: Exploit Protection, M1037: Filter Network Traffic, M1026: Privileged Account Management, M1021: Restrict Web-Based Content
TA-OTHER: Other	T1219: Remote Access Tools	M1038: Execution Prevention, M1037: Filter Network Traffic, M1034: Limit Hardware Installation, M1031: Network Intrusion Prevention, M1042: Disable or Remove Feature or Program
TA-OTHER: Other	T1480: Execution Guardrails	M1055: Do Not Mitigate
TA-OTHER: Other	T1480.001: Environmental Keying	M1055: Do Not Mitigate
TA-OTHER: Other	T1480.002: Mutual Exclusion	M1055: Do Not Mitigate
TA-OTHER: Other	T1484.001: Group Policy Modification	M1047: Audit, M1018: User Account Management, M1026: Privileged Account Management
TA0040: Impact	T1485: Data Destruction	M1032: Multi-factor Authentication, M1053: Data Backup, M1018: User Account Management
TA0040: Impact	T1486: Data Encrypted for Impact	M1040: Behaviour Prevention on Endpoint, M1053: Data Backup
TA0040: Impact	T1489: Service Stop	M1030: Network Segmentation, M1018: User Account Management, M1060: Out-of-Band Communications Channel, M1024: Restrict Registry Permissions, M1022: Restrict File and Directory Permissions
TA0040: Impact	T1490: Inhibit System Recovery	M1038: Execution Prevention, M1028: Operating System Configuration, M1018: User Account Management, M1053: Data Backup
TA0040: Impact	T1491.001: Internal Defacement	M1053: Data Backup
TA0040: Impact	T1529: System Shutdown/Reboot	
TA0010: Exfiltration	T1537: Transfer Data to Cloud Account	M1057: Data Loss Prevention, M1018: User Account Management, M1054: Software Configuration, M1037: Filter Network Traffic
TA0003: Persistence	T1543.003: Windows Service	M1040: Behaviour Prevention on Endpoint, M1028: Operating System Configuration, M1047: Audit, M1045: Code Signing, M1018: User Account Management, M1033: Limit Software Installation, M1026: Privileged Account Management, M1054: Software Configuration, M1022: Restrict File and Directory Permissions

Tactic	Technique	Mitigation
TA0003: Persistence	T1547: Boot or Logon Autostart Execution	
TA0003: Persistence	T1547.004: Winlogon Helper DLL	M1038: Execution Prevention, M1018: User Account Management
TA-OTHER: Other	T1548: Abuse Elevation Control Mechanism	M1038: Execution Prevention, M1028: Operating System Configuration, M1051: Update Software, M1052: User Account Control, M1026: Privileged Account Management, M1018: User Account Management, M1047: Audit, M1022: Restrict File and Directory Permissions
TA-OTHER: Other	T1548.002: Bypass User Account Control	M1051: Update Software, M1047: Audit, M1052: User Account Control, M1026: Privileged Account Management, M1038: Execution Prevention, M1028: Operating System Configuration, M1018: User Account Management, M1022: Restrict File and Directory Permissions
TA-OTHER: Other	T1555.003: Credentials from Web Browsers	M1051: Update Software, M1018: User Account Management, M1017: User Training, M1021: Restrict Web-Based Content, M1027: Password Policies, M1026: Privileged Account Management
TA0009: Collection	T1560.001: Archive via Utility	M1047: Audit
TA-OTHER: Other	T1562.001: Disable or Modify Tools	M1038: Execution Prevention, M1024: Restrict Registry Permissions, M1018: User Account Management, M1022: Restrict File and Directory Permissions, M1047: Audit, M1054: Software Configuration, M1042: Disable or Remove Feature or Program
TA-OTHER: Other	T1562.004: Disable or Modify System Firewall	M1047: Audit, M1018: User Account Management, M1024: Restrict Registry Permissions, M1022: Restrict File and Directory Permissions, M1054: Software Configuration, M1038: Execution Prevention, M1042: Disable or Remove Feature or Program
TA-OTHER: Other	T1562.009: Safe Mode Boot	M1026: Privileged Account Management, M1054: Software Configuration, M1018: User Account Management, M1038: Execution Prevention, M1022: Restrict File and Directory Permissions, M1024: Restrict Registry Permissions, M1047: Audit, M1042: Disable or Remove Feature or Program
TA-OTHER: Other	T1566: Phishing	M1047: Audit, M1031: Network Intrusion Prevention, M1054: Software Configuration, M1021: Restrict Web-Based Content, M1049: Antivirus/Antimalware, M1017: User Training
TA-OTHER: Other	T1566.001: Spearphishing Attachment	M1049: Antivirus/Antimalware, M1018: User Account Management, M1047: Audit, M1031: Network Intrusion Prevention, M1054: Software Configuration, M1017: User Training, M1021: Restrict Web-Based Content

Tactic	Technique	Mitigation
TA-OTHER: Other	T1566.002: Spearphishing Link	M1054: Software Configuration, M1021: Restrict Web-Based Content, M1047: Audit, M1018: User Account Management, M1017: User Training, M1031: Network Intrusion Prevention, M1049: Antivirus/Antimalware
TA0010: Exfiltration	T1567: Exfiltration Over Web Service	M1021: Restrict Web-Based Content, M1057: Data Loss Prevention
TA0010: Exfiltration	T1567.002: Exfiltration to Cloud Storage	M1021: Restrict Web-Based Content, M1057: Data Loss Prevention
TA0002: Execution	T1569.002: Service Execution	M1026: Privileged Account Management, M1040: Behaviour Prevention on Endpoint, M1022: Restrict File and Directory Permissions, M1018: User Account Management
TA-OTHER: Other	T1570: Lateral Tool Transfer	M1037: Filter Network Traffic, M1031: Network Intrusion Prevention
TA-OTHER: Other	T1572: Protocol Tunnelling	M1037: Filter Network Traffic, M1031: Network Intrusion Prevention
TA-OTHER: Other	T1573.001: Symmetric Cryptography	M1031: Network Intrusion Prevention, M1020: SSL/TLS Inspection
TA-OTHER: Other	T1588.005: Exploits	M1056: Pre-compromise
TA0007: Discovery	T1614.001: System Language Discovery	
TA0007: Discovery	T1622: Debugger Evasion	
TA-OTHER: Other	T1650: Acquire Access	M1056: Pre-compromise
TA0007: Discovery	T1652: Device Driver Discovery	

MITRE ATT&CK Mobile TTPs identified for RATs reportedly seen in the EU

Tactic	Technique	Mitigation
TA0009: Collection	T1409: Stored Application Data	M1006: Use Recent OS Version
TA0009: Collection	T1417.001: Keylogging	M1012: Enterprise Policy, M1011: User Guidance, M1006: Use Recent OS Version
TA0009: Collection	T1417.002: GUI Input Capture	M1006: Use Recent OS Version, M1012: Enterprise Policy, M1011: User Guidance
TA0007: Discovery	T1418: Software Discovery	M1011: User Guidance, M1006: Use Recent OS Version
TA0007: Discovery	T1424: Process Discovery	M1006: Use Recent OS Version, M1002: Attestation
TA0007: Discovery	T1426: System Information Discovery	
TA0009: Collection	T1429: Audio Capture	M1006: Use Recent OS Version, M1011: User Guidance
TA0040: Impact	T1471: Data Encrypted for Impact	

TA0009: Collection	T1513: Screen Capture	M1012: Enterprise Policy, M1011: User Guidance, M1013: Application Developer Guidance
TA0009: Collection	T1533: Data from Local System	
TA0040: Impact	T1582: SMS Control	M1011: User Guidance
TA0009: Collection	T1636.003: Contact List	M1011: User Guidance, M1006: Use Recent OS Version

12.2 VULNERABILITIES

Concepts and frameworks used to document vulnerabilities:

CVE Numbering Authority[488]: An authorised entity with specific scope and responsibility to regularly assign CVE IDs and publish corresponding CVE Records. ENISA is a CVE Numbering Authority.

CVE Identifier: The CVE[489] (Common Vulnerabilities and Exposures) programme is an international, community-driven effort to identify and catalogue publicly disclosed vulnerabilities. Each disclosed vulnerability is catalogued within a CVE Record, which includes information about the vulnerability, and is assigned an alphanumeric string that identifies a publicly disclosed vulnerability, called a CVE Identifier (ID). Individual CVE Records are catalogued via the list of CVEs.

EUVD Identifier: Similar to CVE, ENISA assigns and records a unique identifier to each publicly disclosed vulnerability which is catalogued within the EU Vulnerability Database.

CVSS: Common Vulnerability Scoring System[490], is an open framework for communicating the characteristics and severity of vulnerabilities. In the current version (4.0) it uses 4 metrics with numbers between 0 and 10. CVSS adopts the following severity rating based on the score:

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

CWE: The Common Weakness Enumeration[491] is a community-developed list of common software and hardware weakness types that could have security ramifications. A weakness is a condition in a software, firmware, hardware or service component that, under certain circumstances, could contribute to the introduction of vulnerabilities. A CWE is assigned an ID. In many cases, a CWE ID is included in a vulnerability description to enrich the information. This information helps developers to understand common weakness and improve secure development practices.

[488] https://www.cve.org/ResourcesSupport/Glossary
[489] https://www.cve.org/
[490] https://www.first.org/cvss/v4-0/specification-document
[491] https://cwe.mitre.org/index.html

Known Exploited Vulnerability: A KVE is a vulnerability that is officially known as having been exploited during an attack or incident. The US Cybersecurity and Infrastructure Agency (CISA)[492] maintains a catalogue of known exploited vulnerabilities. Organisations should use the KEV catalogue as an input to their vulnerability management prioritisation framework.

Hereunder is a list of vulnerabilities documented as having been exploited in order to target EU organisations in open sources.

CVE	EUVD-ID	CVSS	CWE	PoC	Product	Vendor
CVE-2015-2051	EUVD-2015-2164	10 (v2.0)			D-Link	D-Link DIR-645 Router
CVE-2017-0144	EUVD-2017-0511	8.8 (v3.1)	No info	https://www.exploit-db.com/exploits/42031/; https://www.exploit-db.com/exploits/42030/; https://www.exploit-db.com/exploits/41891/	Microsoft	Windows Smb
CVE-2017-0147	EUVD-2017-0514	7.5 (v3.1)	No info	https://www.exploit-db.com/exploits/41891/; https://www.exploit-db.com/exploits/41987/; https://www.exploit-db.com/exploits/43970/	Microsoft	Windows Smb
CVE-2017-0199	EUVD-2017-0566	7.8 (v3.1)	No info	http://rewtin.blogspot.nl/2017/04/cve-2017-0199-practical-exploitation-poc.html; https://www.exploit-db.com/exploits/41894/; https://www.mdsec.co.uk/2017/04/exploiting-cve-2017-0199-hta-handler-vulnerability/	Microsoft	Microsoft Office (2007–2016)
CVE-2017-11882	EUVD-2017-3478	7.8 (v3.1)	CWE-119	https://github.com/embedi/CVE-2017-11882; https://github.com/unamer/CVE-2017-11882; https://github.com/rxwx/CVE-2017-11882	Microsoft	Microsoft Office
CVE-2017-18368	EUVD-2017-9484	9.8 (v3.1)	CWE-78	https://raw.githubusercontent.com/pedrib/PoC/master/advisories/zyxel_trueonline.txt	ZyXEL	The ZyXEL P660HN-T1A v1
CVE-2018-0802	EUVD-2018-1608	7.8 (v3.1)	CWE-787	https://github.com/rxwx/CVE-2018-0802; https://github.com/zldww2011/CVE-2018-0802_POC	Microsoft	Equation Editor
CVE-2018-0824	EUVD-2018-1629	8.8 (v3.1)	CWE-502	https://www.exploit-db.com/exploits/44906/	N/a	N/a
CVE-2018-10957	EUVD-2018-3009	8.8 (v3.0)	CWE-352	https://packetstormsecurity.com/files/147525/D-Link-DIR-868L-1.12-Cross-Site-Request-Forgery.html	N/a	N/a
CVE-2018-13379	EUVD-2018-5323	9.1 (v3.1)	CWE-22		Fortinet	Fortinet Fortios, Fortiproxy
CVE-2019-0604	EUVD-2019-1370	9.8 (v3.1)	CWE-20		Microsoft	Microsoft Sharepoint Server
CVE-2020-0787	EUVD-2020-2274	7.8 (v3.1)	CWE-59	http://packetstormsecurity.com/files/158056/Background-Intelligent-Transfer-Service-Privilege-Escalation.html	Microsoft	Windows
CVE-2020-1472	EUVD-2020-12346	5.5 (v3.1)	No info	http://packetstormsecurity.com/files/159190/Zerologon-Proof-Of-Concept.html; http://packetstormsecurity.com/files/160127/Zerologon-Netlogon-Privilege-Escalation.html	Microsoft	Windows Server Version 2004
CVE-2020-35730	EUVD-2020-23386	6.1 (v3.1)	CWE-79	https://github.com/roundcube/roundcubemail/compare/1.4.9...1.4.10; https://github.com/roundcube/roundcubemail/releases/tag/1.4.10; https://github.com/roundcube/roundcubemail/releases/tag/1.3.16	Roundcube	Roundcube Webmail
CVE-2021-26084	EUVD-2021-12905	9.8 (v3.1)	CWE-917	http://packetstormsecurity.com/files/167449/Atlassian-Confluence-Namespace-OGNL-Injection.html	Atlassian	Confluence Server
CVE-2021-26855	EUVD-2021-13639	9.1 (v3.1)	CWE-918	http://packetstormsecurity.com/files/161846/Microsoft-Exchange-2019-SSRF-Arbitrary-File-Write.html; http://packetstormsecurity.com/files/161938/Microsoft-Exchange-ProxyLogon-Remote-Code-Execution.html; http://packetstormsecurity.com/files/162610/Microsoft-Exchange-2019-Unauthenticated-Email-Download.html	Microsoft	Microsoft Exchange Server 2016 Cumulative Update 19
CVE-2021-26857	EUVD-2021-13641	7.8 (v3.1)	CWE-502		Microsoft	Microsoft Exchange Server 2016 Cumulative Update 19
CVE-2021-26858	EUVD-2021-13642	7.8 (v3.1)	No info		Microsoft	Microsoft Exchange Server 2019
CVE-2021-27065	EUVD-2021-13836	7.8 (v3.1)	CWE-22	http://packetstormsecurity.com/files/161938/Microsoft-Exchange-ProxyLogon-Remote-Code-Execution.html; http://packetstormsecurity.com/files/162736/Microsoft-Exchange-ProxyLogon-Collector.html	Microsoft	Microsoft Exchange Server 2019
CVE-2021-31207	EUVD-2021-18120	6.6 (v3.1)	CWE-434	http://packetstormsecurity.com/files/163895/Microsoft-Exchange-ProxyShell-Remote-Code-Execution.html	Microsoft	Microsoft Exchange Server 2013 Cumulative Update 23
CVE-2021-33742	EUVD-2021-20419	7.5 (v3.1)	CWE-787		Microsoft	Windows 10 Version 1809
CVE-2021-34473	EUVD-2021-21128	9.1 (v3.1)	CWE-918	http://packetstormsecurity.com/files/163895/Microsoft-Exchange-ProxyShell-Remote-Code-Execution.html	Microsoft	Microsoft Exchange Server 2013 Cumulative Update 23
CVE-2021-34523	EUVD-2021-21177	9.0 (v3.1)	No info	http://packetstormsecurity.com/files/163895/Microsoft-Exchange-ProxyShell-Remote-Code-Execution.html	Microsoft	Microsoft Exchange Server 2013 Cumulative Update 23

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

CVE-2021-4034	EUVD-2021-33934	7.8 (v3.1)	CWE-787	http://packetstormsecurity.com/files/166196/Polkit-pkexec-Local-Privilege-Escalation.html; http://packetstormsecurity.com/files/166200/Polkit-pkexec-Privilege-Escalation.html	N/a	Polkit
CVE-2021-42278	EUVD-2021-29254	7.5 (v3.1)	No info		Microsoft	Windows Server 2019
CVE-2021-44026	EUVD-2021-30885	9.8 (v3.1)	CWE-89	https://github.com/roundcube/roundcubemail/commit/c8947ecb762d9e89c2091bda28d49002817263f1; https://github.com/roundcube/roundcubemail/commit/ee809bde2dcaa04857a919397808a7296681dcfa	Roundcube	Roundcube Webmail
CVE-2022-27924	EUVD-2022-32412	7.5 (v3.1)	CWE-77		N/a	N/a
CVE-2022-3236	EUVD-2022-42644	9.8 (v3.1)	CWE-94		Sophos	Sophos Firewall
CVE-2022-41128	EUVD-2022-44371	8.8 (v3.1)	CWE-787		Microsoft	Windows 10 Version 1809
CVE-2023-20118	EUVD-2023-24297	6.5 (v3.1)	CWE-77		Cisco	Cisco small business routers
CVE-2023-20198	EUVD-2023-24377	10 (v3.1)	CWE-420		Cisco	Cisco IOS XE Software
CVE-2023-22515	EUVD-2023-26655	9.8 (v3.1)	No info	http://packetstormsecurity.com/files/175225/Atlassian-Confluence-Unauthenticated-Remote-Code-Execution.html	Atlassian	Confluence Data Center
CVE-2023-22527	EUVD-2023-26667	9.8 (v3.1)	CWE-74	http://packetstormsecurity.com/files/176789/Atlassian-Confluence-SSTI-Injection.html	Atlassian	Confluence Data Center
CVE-2023-23397	EUVD-2023-27497	9.8 (v3.1)	CWE-20		Microsoft	Microsoft Office LTSC 2021
CVE-2023-27350	EUVD-2023-31126	9.8 (v3.1)	CWE-284	http://packetstormsecurity.com/files/171982/PaperCut-MF-NG-Authentication-Bypass-Remote-Code-Execution.html; http://packetstormsecurity.com/files/172022/PaperCut-NG-MG-22.0.4-Authentication-Bypass.html; https://news.sophos.com/en-us/2023/04/27/increased-exploitation-of-papercut-drawing-blood-around-the-internet/	Papercut	Ng
CVE-2023-27532	EUVD-2023-31287	7.5 (v3.1)	CWE-306		N/a	Veeam Backup & Replication
CVE-2023-28461	EUVD-2023-32140	9.8 (v3.1)	CWE-287		N/a	N/a
CVE-2023-34048	EUVD-2023-38166	9.8 (v3.1)	CWE-787		Vmware	Vmware Vcenter Server
CVE-2023-3519	EUVD-2023-44176	9.8 (v3.1)	CWE-94	http://packetstormsecurity.com/files/173997/Citrix-ADC-NetScaler-Remote-Code-Execution.html	Citrix	Netscaler Adc
CVE-2023-38831	EUVD-2023-42604	7.8 (v3.1)	CWE-345	https://www.bleepingcomputer.com/news/security/winrar-zero-day-exploited-since-april-to-hack-trading-accounts/; http://packetstormsecurity.com/files/174573/WinRAR-Remote-Code-Execution.html; https://blog.google/threat-analysis-group/government-backed-actors-exploiting-winrar-vulnerability/	WinRAR	RARLAB WinRAR
CVE-2023-42793	EUVD-2023-47222	9.8 (v3.1)	CWE-288	http://packetstormsecurity.com/files/174860/JetBrains-TeamCity-Unauthenticated-Remote-Code-Execution.html; https://www.securityweek.com/recently-patched-teamcity-vulnerability-exploited-to-hack-servers/	Jetbrains	Teamcity
CVE-2023-43770	EUVD-2023-48147	6.1 (v3.1)	CWE-79	https://github.com/roundcube/roundcubemail/commit/e92ec206a886461245e1672d8530cc93c618a49b	N/a	N/a
CVE-2023-46604	EUVD-2023-2719	10.0 (v3.1)	CWE-502	https://packetstormsecurity.com/files/175676/Apache-ActiveMQ-Unauthenticated-Remote-Code-Execution.html	Apache Software Foundation	Apache Activemq
CVE-2023-46747	EUVD-2023-50916	9.8 (v3.1)	CWE-288	http://packetstormsecurity.com/files/175673/F5-BIG-IP-TMUI-AJP-Smuggling-Remote-Command-Execution.html; https://www.secpod.com/blog/f5-issues-warning-big-ip-vulnerability-used-in-active-exploit-chain/	F5	Big-ip
CVE-2023-48788	EUVD-2023-52821	9.8 (v3.1)	CWE-89		Fortinet	Forticlientems
CVE-2024-0012	EUVD-2024-15815	9.3 (v4.0)	CWE-306		Palo Alto Networks	Cloud Ngfw
CVE-2024-20399	EUVD-2024-18114	6.0 (v3.1)	CWE-78	https://www.sygnia.co/threat-reports-and-advisories/china-nexus-threat-group-velvet-ant-exploits-cisco-0-day/	Cisco	Cisco Nx-os Software
CVE-2024-21287	EUVD-2024-19000	7.5 (v3.1)	CWE-863		Oracle Corporation	Oracle Agile Plm Framework
CVE-2024-21338	EUVD-2024-19050	7.8 (v3.1)	CWE-822	https://www.exploit-db.com/exploits/52275	Microsoft	Windows 10 Version 1809
CVE-2024-21412	EUVD-2024-19121	8.1 (v3.1)	CWE-693		Microsoft	Windows 11 Version 21h2
CVE-2024-21762	EUVD-2024-19376	9.8 (v3.1)	CWE-787		Fortinet	Fortiproxy
CVE-2024-24919	EUVD-2024-22282	8.6 (v3.1)	CWE-200	https://www.mnemonic.io/resources/blog/advisory-check-point-remote-access-vpn-vulnerability-cve-2024-24919/	Checkpoint	Check Point Quantum Gateway, Spark Gateway And Cloudguard Network
CVE-2024-27198	EUVD-2024-24437	9.8 (v3.1)	CWE-288	https://www.darkreading.com/cyberattacks-data-breaches/jetbrains-teamcity-mass-exploitation-underway-rogue-accounts-thrive	Jetbrains	Teamcity
CVE-2024-27348	EUVD-2024-1059	9.8 (v3.1)	No info		Apache Software Foundation	Apache Hugegraph-server

CVE-2024-28986	EUVD-2024-26048	9.8 (v3.1)	CWE-502		Solarwinds	Web Help Desk
CVE-2024-30088	EUVD-2024-28025	7.0 (v3.1)	CWE-367		Microsoft	Windows 10 Version 1809
CVE-2024-3400	EUVD-2024-31989	10.0 (v3.1)	CWE-20	https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/	Palo Alto Networks	Pan-os
CVE-2024-34102	EUVD-2024-2102	9.8 (v3.1)	CWE-611		Adobe	Adobe Commerce
CVE-2024-36401	EUVD-2024-2280	9.8 (v3.1)	CWE-95	https://github.com/geoserver/geoserver/security/advisories/GHSA-6jj6-gm7p-fcvv; https://github.com/geotools/geotools/security/advisories/GHSA-w3pj-wh35-fq8w; https://github.com/geotools/geotools/pull/4797	Geoserver	Geoserver
CVE-2024-37085	EUVD-2024-36416	6.8 (v3.1)	CWE-287		N/a	Vmware Esxi
CVE-2024-37383	EUVD-2024-36625	6.1 (v3.1)	CWE-79	https://github.com/roundcube/roundcubemail/commit/43aaaa528646877789ec028d87924ba1accf5242; https://github.com/roundcube/roundcubemail/releases/tag/1.6.7; https://github.com/roundcube/roundcubemail/releases/tag/1.5.7	N/a	N/a
CVE-2024-38014	EUVD-2024-37504	7.8 (v3.1)	CWE-269		Microsoft	Windows 10 Version 1809
CVE-2024-38094	EUVD-2024-37782	7.2 (v3.1)	CWE-502		Microsoft	Microsoft Sharepoint Enterprise Server 2016
CVE-2024-38178	EUVD-2024-37148	7.5 (v3.1)	CWE-843		Microsoft	Windows 11 Version 24h2
CVE-2024-38213	EUVD-2024-37180	6.5 (v3.1)	CWE-693		Microsoft	Windows 10 Version 1809
CVE-2024-38226	EUVD-2024-37192	7.3 (v3.1)	CWE-693		Microsoft	Microsoft Office 2019
CVE-2024-38475	EUVD-2024-37356	9.1 (v3.1)	CWE-116	https://www.blackhat.com/us-24/briefings/schedule/index.html#confusion-attacks-exploiting-hidden-semantic-ambiguity-in-apache-http-server-pre-recorded-40227; https://github.com/apache/httpd/commit/9a6157d1e2f7ab15963020381054b48782bc18cf	Apache Software Foundation	Apache HTTP Server
CVE-2024-38812	EUVD-2024-37703	9.8 (v3.1)	CWE-122		N/a	Vmware Vcenter Server
CVE-2024-38813	EUVD-2024-37704	7.5 (v3.1)	CWE-250		N/a	Vmware Vcenter Server
CVE-2024-38856	EUVD-2024-37643	9.8 (v3.1)	CWE-863		Apache Software Foundation	Apache Ofbiz
CVE-2024-40711	EUVD-2024-38578	9.8 (v3.1)	CWE-502		Veeam	Backup And Recovery
CVE-2024-42009	EUVD-2024-39391	9.3 (v3.1)	CWE-79	https://github.com/roundcube/roundcubemail/releases; https://github.com/roundcube/roundcubemail/releases/tag/1.5.8; https://github.com/roundcube/roundcubemail/releases/tag/1.6.8	N/a	N/a
CVE-2024-43047	EUVD-2024-40024	7.8 (v3.1)	CWE-416		Qualcomm, Inc.	Snapdragon
CVE-2024-43451	EUVD-2024-40720	6.5 (v3.1)	CWE-73		Microsoft	Windows Server 2025
CVE-2024-45195	EUVD-2024-41762	7.5 (v3.1)	CWE-425		Apache Software Foundation	Apache Ofbiz
CVE-2024-45519	EUVD-2024-41520	10.0 (v3.1)	No info	https://blog.projectdiscovery.io/zimbra-remote-code-execution/	N/a	N/a
CVE-2024-50302	EUVD-2024-44804	5.5 (v3.1)	CWE-908		Linux	Linux
CVE-2024-50623	EUVD-2024-45217	9.8 (v3.1)	CWE-434		N/a	N/a
CVE-2024-53104	EUVD-2024-51776	7.8 (v3.1)	CWE-787		Linux	Linux
CVE-2024-7971	EUVD-2024-48804	9.6 (v3.1)	CWE-843	https://www.microsoft.com/en-us/security/blog/2024/08/30/north-korean-threat-actor-citrine-sleet-exploiting-chromium-zero-day/	Google	Chrome
CVE-2024-8190	EUVD-2024-49004	7.2 (v3.1)	CWE-78		Ivanti	Cloud Services Appliance (CSA)
CVE-2024-8963	EUVD-2024-49510	9.4 (v3.1)	CWE-22		Ivanti	Cloud Services Appliance (CSA)
CVE-2024-9380	EUVD-2024-49898	7.2 (v3.1)	CWE-77		Ivanti	Cloud Services Appliance (CSA)
CVE-2024-9474	EUVD-2024-50354	6.9 (v4.0)	CWE-78	https://github.com/k4nfr3/CVE-2024-9474	Palo Alto Networks	Cloud Ngfw
CVE-2024-9680	EUVD-2024-50087	9.8 (v3.1)	CWE-416		Mozilla	Firefox

CVE-2025-0108	EUVD-2025-1505	8.8 (v4.0)	CWE-306	https://github.com/iSee857/CVE-2025-0108-PoC; https://www.darkreading.com/remote-workforce/patch-now-cisa-researchers-warn-palo-alto-flaw-exploited-wild; https://www.securityweek.com/palo-alto-networks-confirms-exploitation-of-firewall-vulnerability/	Palo Alto Networks	Cloud NGFW
CVE-2025-0282	EUVD-2025-1580	9.0 (v3.1)	CWE-121	https://labs.watchtowr.com/exploitation-walkthrough-and-techniques-ivanti-connect-secure-rce-cve-2025-0282/; https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search_api_fulltext=CVE-2025-0282; https://github.com/sfewer-r7/CVE-2025-0282	Ivanti	Connect Secure
CVE-2025-0411	EUVD-2025-1658	7.0 (v3.1)	CWE-693		7-zip	7-zip
CVE-2025-20188	EUVD-2025-13907	10 (v3.1)	CWE-798	https://horizon3.ai/attack-research/attack-blogs/cisco-ios-xe-wlc-arbitrary-file-upload-vulnerability-cve-2025-20188-analysis/	Cisco	Cisco IOS XE Software
CVE-2025-21590	EUVD-2025-6303	6.7 (v4.0)	CWE-653		Juniper Networks	Junos Os
CVE-2025-22457	EUVD-2025-9646	9 (v3.1)	CWE-121		Ivanti	Ivanti Connect Secure
CVE-2025-24054	EUVD-2025-6336	6.5 (v3.1)	CWE-73		Microsoft	Windows 10
CVE-2025-24200	EUVD-2025-3671	4.6 (v3.1)	CWE-863		Apple	iPadOS
CVE-2025-24989	EUVD-2025-4642	8.2 (v3.1)	CWE-284		Microsoft	Microsoft Power Pages
CVE-2025-26633	EUVD-2025-6311	7.0 (v3.1)	CWE-707		Microsoft	Windows 10 Version 1809
CVE-2025-27363	EUVD-2025-6367	8.1 (v3.1)	CWE-787		Freetype	Freetype
CVE-2025-2783	EUVD-2025-8225	8.3 (v3.1)	No info		Google	Chrome
CVE-2025-29824	EUVD-2025-10122	7.8 (v3.1)	CWE-416		Microsoft	Windows Server 2019
CVE-2025-30406	EUVD-2025-9671	9 (v3.1)	CWE-321		Gladinet	CentreStack
CVE-2025-31161	EUVD-2025-9910	9.8 (v3.1)	CWE-305	https://www.darkreading.com/vulnerabilities-threats/disclosure-drama-clouds-crushftp-vulnerability-exploitation; https://www.huntress.com/blog/crushftp-cve-2025-31161-auth-bypass-and-post-exploitation; https://www.infosecurity-magazine.com/news/crushftp-flaw-exploited-disclosure/	CrushFTP	CrushFTP
CVE-2025-31324	EUVD-2025-11987	10 (v3.1)	CWE-434	https://onapsis.com/blog/active-exploitation-of-sap-vulnerability-cve-2025-31324/; https://www.bleepingcomputer.com/news/security/sap-fixes-suspected-netweaver-zero-day-exploited-in-attacks/	SAP	SAP NetWeaver
CVE-2025-32433	EUVD-2025-11793	10 (v3.1)	CWE-306	https://github.com/erlang/otp/security/advisories/GHSA-37cp-fgq5-7wc2; https://github.com/erlang/otp/commit/0fcd9c56524b28615e8ece65fc0c3f66ef6e4c12; https://github.com/erlang/otp/commit/6eef04130afc8b0ccb63c9a0d8650209cf54892f	Erlang	OTP
CVE-2025-32756	EUVD-2025-14705	9.6 (v3.1)	CWE-121		Fortinet	FortiVoice, FortiRecorder, FortiMail, FortiNDR, FortiCamera
CVE-2025-33053	EUVD-2025-17721	8.8 (v3.1)	CWE-73	https://www.darkreading.com/vulnerabilities-threats/stealth-falcon-apt-exploits-microsoft-rce-zero-day-mideast; https://www.bleepingcomputer.com/news/security/stealth-falcon-hackers-exploited-windows-webdav-zero-day-to-drop-malware/	Microsoft	Windows 10
CVE-2025-33073	EUVD-2025-17737	8.8 (v3.1)	CWE-284		Microsoft	Windows Server 2019
CVE-2025-37899	-	4.7 (v3.1)			Linux	Linux
CVE-2025-43200	EUVD-2025-18428	4.8 (v3.1)	No info		Apple	iOS & iPadOS
CVE-2025-4427	EUVD-2025-14388	5.3 (v3.1)	CWE-288		Ivanti	Endpoint Manager Mobile
CVE-2025-4428	EUVD-2025-14387	7.2 (v3.1)	CWE-94		Ivanti	Endpoint Manager Mobile
CVE-2025-4664	EUVD-2025-14909	4.3 (v3.1)	No info		Google	Chrome
CVE-2025-49113	EUVD-2025-16605	9.9 (v3.1)	CWE-502	https://github.com/roundcube/roundcubemail/pull/9865; https://github.com/roundcube/roundcubemail/releases/tag/1.6.11; https://github.com/roundcube/roundcubemail/commit/0376f69e958a8fef7f6f09e352c541b4e7729c4d	Roundcube	Roundcube Webmail
CVE-2025-5419	EUVD-2025-16695	8.8 (v3.1)	CWE-125		Google	Chrome
CVE-2025-5777	EUVD-2025-18497	9.3 (v4.0)	CWE-125	https://doublepulsar.com/citrixbleed-2-exploitation-started-mid-june-how-to-spot-it-f3106392aa71; https://www.bleepingcomputer.com/news/security/cisa-tags-citrix-bleed-2-as-exploited-gives-agencies-a-day-to-patch/	Citrix	NetScaler
CVE-2025-6019	EUVD-2025-18685	7 (v3.1)	CWE-250		RedHat	Red Hat Enterprise Linux 10
CVE-2025-6543	EUVD-2025-19085	9.2 (v4.0)				

12.3 LEXICON

Term	Definition
Attribution	A political determination linking cyber activity to a specific actor or group based on technical and intelligence evidence.
Click-fix	A social engineering tactic tricking users into clicking links to 'fix' fake security issues, often leading to malware.
CNA	CVE Numbering Authority, an entity authorised to assign CVE identifiers for vulnerabilities.
CVE	Common Vulnerabilities and Exposures, a reference system for publicly disclosed security flaws.
CVSS	Common Vulnerability Scoring System, a standardised framework for rating software vulnerabilities.
CWE	Common Weakness Enumeration, a classification of software weaknesses that can lead to vulnerabilities.
Cyber incident	An event that compromises the integrity, confidentiality or availability of information systems, networks, or data.
Data breach	An incident where sensitive, protected or confidential data is accessed or disclosed without authorisation.
EUVD-ID	European Vulnerability Database Identifier, a unique identifier for vulnerabilities in the EU context.
Faketivism	Impersonation of a hacktivist persona.
IAB	Initial Access Broker, a threat actor who sells or trades access to compromised systems.
Imputation	A provisional association of cyber activity with an intrusion set, based on technical indicators (aka technical attribution).
IMS	Intrusion Manipulation Set, operators of information operations, FIMI.
Infostealer	Malware designed to steal sensitive information such as credentials, banking data or system details.
Intrusion set	A cluster of related intrusion activity imputed to a single threat actor or campaign over time.
Malspam	Email campaigns that distribute malicious attachments or links to deliver malware.
Malvertising	Use of malicious online advertisements to distribute malware or redirect users to harmful sites.
Moonlighting	Employees conducting unauthorised cyber activities or side job, possibly for financial gain.
Quishing	QR code-based phishing attacks that direct victims to malicious websites or payloads.
State-aligned	An intrusion set or campaign whose objectives allegedly align with a state's interests, without formal state control.
State-nexus	An intrusion set or campaign with alleged direct operational or strategic ties to a nation-state.
Supply-chain attack	A cyberattack exploiting vulnerabilities in suppliers or service providers to compromise downstream entities.
Third-party attack	An attack that compromises a partner, supplier or vendor to target another organisation.
Vishing	A phishing attack conducted over voice calls to trick victims into revealing sensitive information.
Zero-day vulnerability	A previously unknown flaw in software or hardware exploited before a fix is available.

13. LOG HISTORY

Date	Edit
December 2025	References edited
January 2026	References edited

XX-00-00-000-XX-X

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

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

ISBN 978-92-9204-723-8
DOI: 10.2824/1946374