CERT-EU

THREAT LANDSCAPE REPORT

2025

A YEAR IN REVIEW

VERSION 1 – 8 APRIL 2026

CERT-EU, The Cybersecurity Service for Union entities

This page is left intentionally blank.

Table of Contents

1 About CERT-EU

CERT-EU is the Cybersecurity Service for the European Union institutions, bodies, offices and agencies (Union entities). Our legal basis is Regulation (EU) No 2023/2841 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (OJ L, 2023/2842, 18.12.2023) (the 'Cybersecurity Regulation').

We were established in 2011. **In 2026, we are celebrating our 15th anniversary!**

2 Key findings

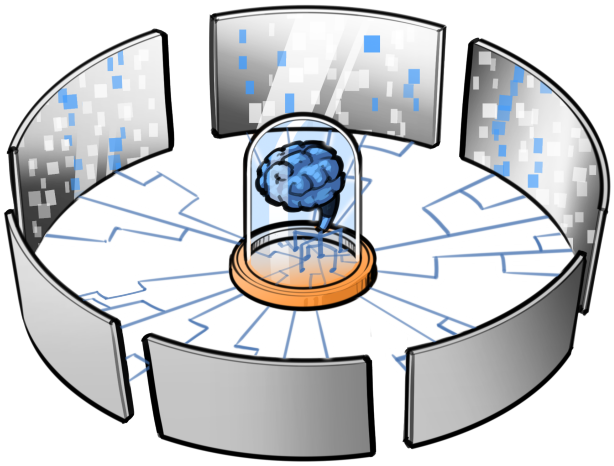
In 2025, we analysed cyber threats to support our constituents, the Union entities, in detecting and protecting against cyberattacks. Here are our key findings.

1. Global events occurring in 2025, such **as conferences and summits, elections, conflicts, and sanctions were once again catalysts for cyberattacks** against Union entities and their ecosystem. Threat actors either weaponised the events as social engineering bait, singled out attendees as high-value targets, or launched cyberattacks in support of their wider strategic objectives.
2. In 2025, we identified at least 174 distinct actors who engaged in malicious activities of interest against Union entities or their ecosystem.[1] Notably, **our constituency had critical exposure to five threat actors**, high exposure to 34, medium exposure to 83, and low exposure to 52 threat actors. The fall in critical exposure compared with last year – from 20 to 5 – mirrors the decrease in significant incidents (see finding 6 below).
3. **Cyberespionage & prepositioning accounted for the largest share at 38%** of recorded activity. Our expanded monitoring through automation and artificial intelligence (AI) increased our visibility into cybercrime and opportunistic activity, which likely accounts for the higher share of these categories compared to 2024.
4. Malicious activities of interest that could be linked to a country of origin, based on information from reliable sources, were most often associated with the **People's Republic of China** (China), closely followed by the **Russian Federation** (Russia). Threat actors linked to China primarily exploited vulnerabilities and supply-chain compromises, while threat actors linked to Russia heavily targeted entities supporting Ukrainian efforts.
5. Threat actors **increasingly leveraged AI** to enhance social engineering campaigns, including voice cloning, personalised phishing content, and deepfakes of officials. In a notable development, a reportedly China-linked threat actor directed a jailbroken **agentic AI system** against entities in the technology, finance, manufacturing, and government sectors, achieving autonomous intrusion in a small number of cases.
6. In 2025, **exploitation of vulnerable internet-facing software was the initial access vector with the highest impact**, a trend that continued from previous years. Spoofing and impersonation tactics rose in frequency, while credential theft remained consistent.
7. CERT-EU responded to **nine significant incidents**[2] in 2025, down from 15 in 2024. Vulnerability exploitation was the initial access vector in seven of these incidents, including two **zero-day compromises.** In one case, the intrusion resulted from the **compromise of a service provider** with access to a Union entity's internal systems. The cause for this decrease is unclear, but we do not interpret it as a reduction in threats or an indicator of improved defences.
8. Within our ecosystem, **the defence sector was most targeted**, followed by finance and diplomacy. Compared to 2024, the transport sector dropped from second to fifth place, as finance, diplomacy, and technology received increased targeting.
9. We recorded 178 cases of **MAI against 90 partner organisations** in 2025. Although the impact on Union entities varied, none escalated into a significant incident. Public administration was the most frequently targeted partner category.

[1] As defined in the CERT-EU Cyber Threat Intelligence Framework, the ecosystem is a set of components that reflect the exposure of Union entities to supply-chain risks, geopolitical developments, regional threats, and risks related to their business activity. These components include countries of operation, sectors of activity, geopolitical events of interest, partners, providers, systems and software. See: https://cert.europa.eu/publications/threat-intelligence/cyber-threat-intelligence-framework/ - ecosystem.

[2] For more information on reporting obligations concerning significant incidents, see Article 21 of Regulation (EU) No 2023/2841.

10. Successful **intrusions into telecommunication** providers were recurrent**,** though not widespread, and carry significant downstream risk.
11. Our analysis identified **198 software products used by Union entities that were targeted or exploited** in 2025, up from 110 in 2024. The most frequently exploited categories included content management tools, development environments, and edge devices.



3 Methodology and scope

This report is based on analysis of **Malicious Activity of Interest (MAI)** data collected throughout 2025. For details on what we consider MAI, please read the Cyber Threat Intelligence Framework published on our website.[3]

The dataset reflects our collection priorities and the availability of information. Our own telemetry provides greater visibility into threats targeting Union entities than third-party disclosures do for the broader ecosystem. We also assign higher collection priority to cyberespionage and public-facing software exploitation, given their impact on our constituents.

In 2025, we significantly expanded our use of automation and artificial intelligence (AI) in our monitoring and analysis processes. This broadened our detection reach and enabled us to process a larger volume of malicious activity than in previous years. As a result, year-on-year increases in certain metrics – such as the number of tracked threat actors, software products, and the share of cybercrime and opportunistic activity – partly reflect this expanded monitoring capability rather than a proportional increase in threats. This methodological change should be considered when interpreting comparisons with 2024 data[4].

- **Union entities accounted for 25% of total MAI in our dataset.** The remaining 75% related to our ecosystem.
- 33% of the activity was tracked because it involved software used by Union entities.
- Cyberespionage & prepositioning represented the largest share at 38%, followed by cybercrime at 30%.

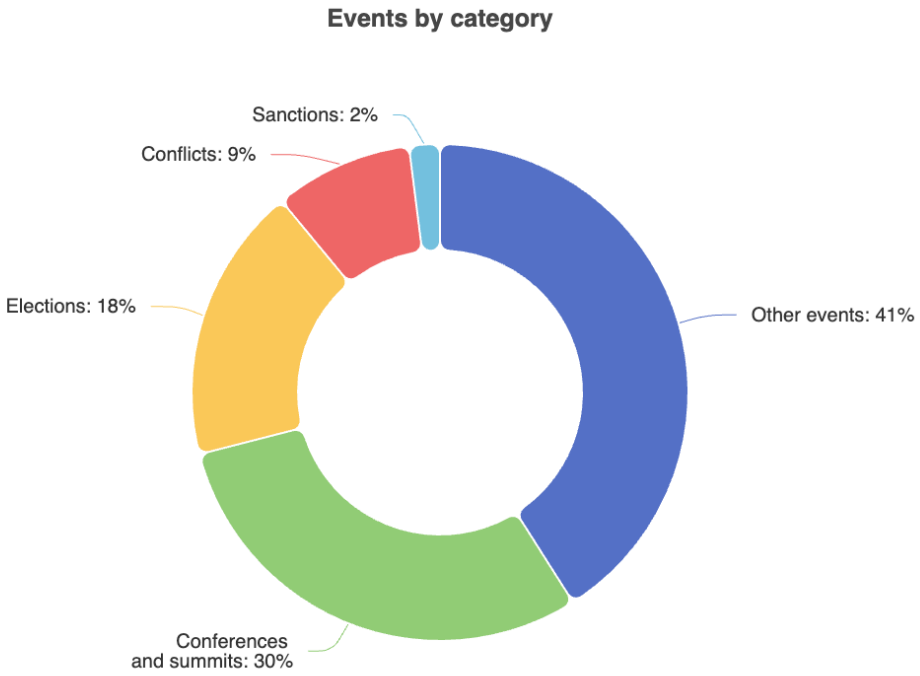
4 Global events

In 2025, cyberattacks continued to be shaped by geopolitical developments. Threat actors used **global events as lures in social engineering campaigns and as triggers for reactive cyber operations** such as hacktivism and digital foreign interference.

We analysed 44 distinct events linked to MAI in our ecosystem. These events were categorised as conferences and summits (30%), elections (18%), conflicts (9%), and sanctions (2%). The remaining 41% related to other events such as major sports events, civil unrest and protests, holiday periods, tensions between countries, and policy decisions on sensitive topics such as EU accession talks or support to Ukraine.

[3] For details on what we consider MAI affecting Union entities and our ecosystem, please refer our Cyber Threat Intelligence Framework, available at https://cert.europa.eu/publications/threat-intelligence/cyber-threat-intelligence-framework/.

[4] The 2024 threat landscape report can be consulted at https://cert.europa.eu/publications/threat-intelligence/tlr2024/pdf.



Summits and conferences

High-level events such as **political summits and industry conferences** were direct targets of cyberattacks. Threat actors also abused them as lures in social engineering campaigns. Cyberespionage actors sent spearphishing e-mails using **fake invitations** or documents themed around these events, capitalising on the fact that individuals from specific sectors were gathering in one location. For example, Russia-linked threat actors reportedly targeted participants of the December "Brussels Indo-Pacific Dialogue" with phishing to steal their credentials.[5]

Supposed hacktivists frequently carried out Distributed Denial-of-Service (DDoS) attacks on websites linked to high-level events or on entities in the host country. For example, during the June NATO summit held in the Netherlands, pro-Russia supposed hacktivists claimed DDoS attacks on the websites of Dutch municipalities and organisations.[6]

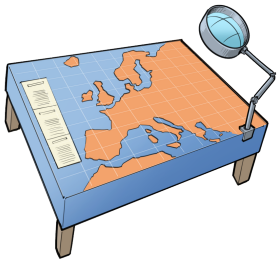
Elections

State-sponsored threat actors conducted cyber operations **targeting at least eight national elections** in EU and neighbouring countries in 2025. Most elections were accompanied by DDoS attacks from pro-Russia supposed hacktivists, typically occurring shortly before or on election day. These attacks targeted political party websites and entities in sectors such as transportation, energy, and media, likely to amplify the perception of disruption. For example, during the Danish regional elections in November, pro-Russia supposed hacktivists targeted the websites of four political parties and The Copenhagen Post with DDoS attacks. Similarly, amid the Romanian elections in May, pro-Russia supposed hacktivists claimed responsibility for DDoS attacks against at least four Romanian presidential candidates' websites.

[5] https://www.volexity.com/blog/2025/12/04/dangerous-invitations-russian-threat-actor-spoofs-european-security-events-in-targeted-phishing-attacks/
[6] https://apnews.com/article/nato-summit-cybersecurity-hack-russia-netherlands-fa97bbf8797a51c2885d47f5f83691be

Threat actors regularly used digital foreign interference campaigns when targeting elections, **seeking to influence electorates.** For example, in the context of the Polish national elections, the Russia-aligned Doppelgänger campaign disseminated false narratives on social media, aimed at eroding public confidence in the Polish government and NATO.

Conflicts



Major conflicts such as Russia's war on Ukraine and the Israel-Hamas conflict spilled over into cyberspace. Threat actors conducted cyberespionage, destructive attacks, digital foreign interference, and hacktivist attacks against perceived adversaries and their allies to advance their strategic objectives.

DDoS attacks and attacks targeting internet-exposed industrial control systems were typically carried out by **supposed hacktivist groups seeking to exert political pressure or amplify narratives aligned with a party to the conflict.** For instance, the military escalation between the Islamic Republic of Iran (Iran), the State of Israel (Israel), and the United States of America (the US) in June 2025 triggered a surge in both pro-Israel and pro-Iran supposed hacktivist claims targeting civil society and government entities across Europe. These groups typically exaggerated the impact of their operations to sow fear and erode trust in public institutions.

Destructive attacks, such as wipers, were rarely observed outside the direct context of armed conflict, where they were used as tools of cyberwarfare alongside kinetic operations. For example, Russia-linked threat actor Sandworm deployed wipers against entities in Ukraine's public administration, energy, transport, and agriculture sectors.[7] In a rare instance within the ecosystem of our constituency, **a Polish renewable energy operator experienced an attempted wiper attack** in late December,[8] with no reported disruption to the national energy supply. The attack was attributed to Sandworm by ESET.[9]

Sanctions

When the EU issued decisions on sanctions, we typically observed an uptick in cyberattacks linked to the entity or country being sanctioned. In October 2025, the **EU issued the 19th sanctions package on Russia** relating to its ongoing invasion of Ukraine.[10] The sanctions package coincided with Russia-aligned Doppelgänger activity conducting digital foreign interference in the EU. The campaign used domains that mimicked legitimate media entities and government institutions. It portrayed Ukraine and its Western European allies in a negative light and focused on the supposed decline of Western influence.

Other events

The remaining 41% related to other events that do not fall in the above four categories. Other events included major sports and cultural events, civil unrest and protests, holiday periods, tensions between countries, and policy decisions on sensitive topics like EU accession or **expressions of support for a country at war**. A few examples.

- In July, the European Parliament re-elected Ursula von der Leyen as the President of the European Commission.[11] This event coincided with a spike in Russia-aligned digital foreign interference on social media.[12]

[7] https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q2-2025-q3-2025.pdf
[8] https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/
[9] https://www.welivesecurity.com/en/eset-research/eset-research-sandworm-cyberattack-poland-power-grid-late-2025/
[10] https://www.consilium.europa.eu/en/press/press-releases/2025/10/23/19th-package-of-sanctions-against-russia-eu-targets-russian-energy-third-country-banks-and-crypto-providers/
[11] https://www.europarl.europa.eu/doceo/document/CRE-10-2024-07-18_EN.html
[12] https://english.elpais.com/international/2025-07-22/russia-used-the-vote-of-no-confidence-against-von-der-leyen-to-stir-up-polarization-in-the-eu.html

- In May, pro-Palestine supposed hacktivists referred to the European Song Contest and simultaneously claimed DDoS attacks against Union entities.[13] The increase in traffic to the Union entity websites could be observed but caused no downtime.
- In December, Finland and Ukraine closed the "Agreement on security cooperation and long-term support between the Republic of Finland and Ukraine".[14] This coincided with a DDoS campaign dubbed #OpFinland by pro-Russia supposed hacktivists.

5 Threat Actors

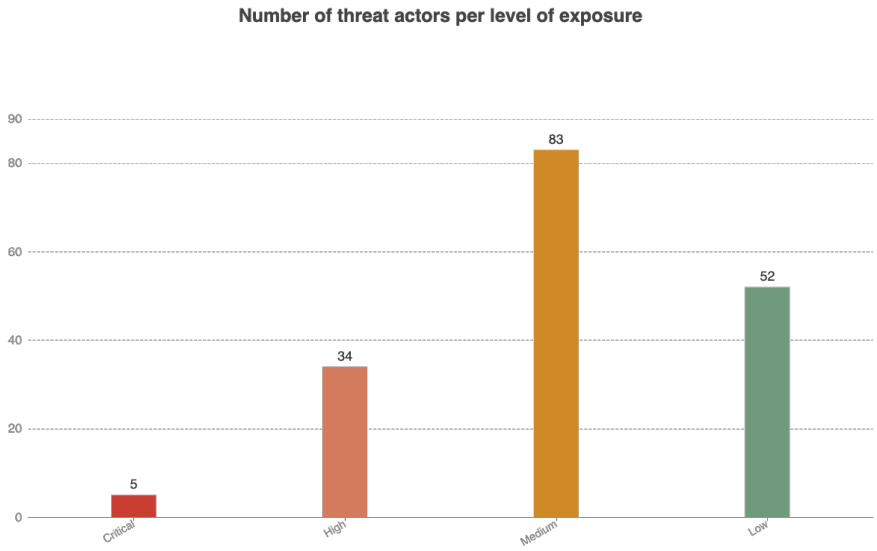
In 2025, we identified at least **174 distinct malicious actors who engaged in MAI against Union entities** or their ecosystem. This represents a significant increase from the 110 threat actors identified in 2024.

Exposure

We ranked the level of exposure of our constituency to these actors from critical to low.

Our constituency had critical exposure to five threat actors, high exposure to 34, medium exposure to 83, and low exposure to 52 threat actors. The fall in critical exposure compared with last year (from 20 to 5) mirrors the decrease in significant incidents.

Certain threat actors engaged in several activities that led to different levels of exposure. For example, an unsuccessful spearphishing attack (high exposure) and, at a different time, activity targeting at least two elements of Union entities' ecosystem (medium exposure). In such a case, we have assigned the highest threat level to that actor (high exposure).



Critical exposure

We identified five threat actors to whom our constituency had critical exposure. **These threat actors conducted cyberattacks which caused significant incidents at Union entities**. We were able to link some of the breaches to known threat actors, while others remained unidentified.[15] We handled nine significant incidents, but several related to the same threat actor, which explains why only five are listed under critical exposure. We highlight two below.

[13] https://www.eurovision.com/eurovision-song-contest/basel-2025/

[14] https://www.presidentti.fi/en/agreement-on-security-cooperation-and-long-term-support-between-the-republic-of-finland-and-ukraine/

[15] In this case, we refer to them as Unidentified Threat Actors (UTAs) and we give them a number such as UTA-76.

UTA-67. An unknown threat actor responsible for breaching two FortiGate firewalls of a Union entity, highly likely through exploitation of a remote code execution vulnerability.

UTA-76. Another unknown threat actor successfully exploited two zero-day vulnerabilities in Ivanti Endpoint Manager Mobile (EPMM), a mobile device management solution.

High exposure

We identified 34 threat actors to whom our constituency had high exposure. These threat actors targeted one or more Union entities without causing a significant incident. For example, several threat actors sent spearphishing e-mails that were detected and blocked by Union entities, or the adversaries attempted but failed to exploit exposed software products. We highlight two below.

Mustang Panda. Throughout 2025, this **China-linked threat actor** demonstrated a sustained interest in European diplomatic entities through targeted spearphishing campaigns. Their technical approach remained centred on Dynamic Link Library (DLL) side-loading.[16] In one campaign, the actor leveraged this method alongside a decoy document masquerading as an official European Commission meeting agenda to lure targets into initiating the infection chain.[17]

UTA-78. We track UTA-78 as responsible for large-scale zero-day exploitation of Microsoft SharePoint vulnerabilities dubbed ToolShell. Microsoft links ToolShell exploitation to three China-linked threat actors: Linen Typhoon, Violet Typhoon, and Storm-2603.[18] We currently withhold judgement on possible overlap and instead track this activity targeting Union entities as UTA-78. We observed the more advanced and stealthier variant of the exploit, tracked as NoShell by SentinelOne,[19] at one Union entity.

Medium exposure

We identified 83 threat actors to whom our constituency had medium exposure. We highlight two below.

APT28. In 2025, the **Russia-linked APT28** targeted Western logistics and technology firms involved in coordinating aid to Ukraine. The group conducted credential harvesting and exploited edge devices like IP cameras.[20]

Salt Typhoon. The **China-aligned threat actor** reportedly compromised a European telecommunications provider in July 2025 by exploiting a vulnerability in Citrix NetScaler Gateway appliances.[21] The actor used DLL side-loading through legitimate antivirus software to deliver a custom backdoor and maintain stealthy access within the target network.

Low exposure

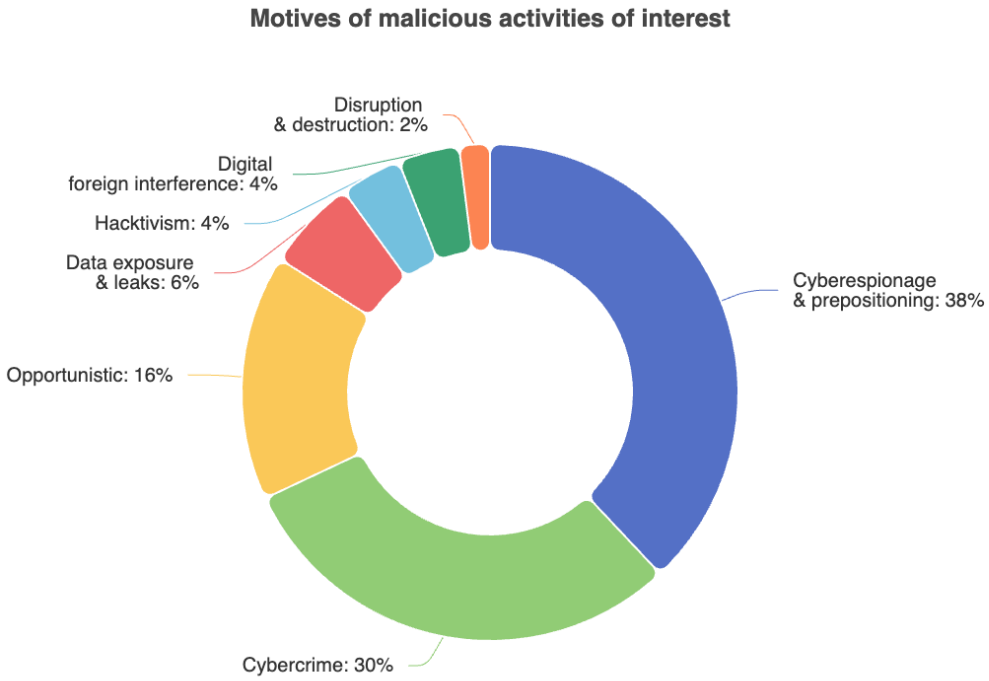
We identified 52 threat actors to whom our constituency had low exposure. They were responsible for at least one MAI affecting exactly one element of the ecosystem during the period of interest. 52 represents a modest increase from the 47 identified last year.

Motives

When examining MAI, we categorised each attack based on the inferred motives of the threat actor. While this classification is not an exact science, it takes into account several factors, including the apparent objective of the attack, the identity of the attacker, the profile of the targeted victims, and the sophistication and persistence of the observed behaviour.

In 2025, **38% of the recorded activity was categorised as cyberespionage & prepositioning.** 30% of MAI activity was classified as cybercrime, while 16% was deemed opportunistic.

[16] https://cloud.google.com/blog/topics/threat-intelligence/prc-nexus-espionage-targets-diplomats
[17] https://arcticwolf.com/resources/blog/unc6384-weaponizes-zdi-can-25373-vulnerability-to-deploy-plugx/
[18] https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/
[19] https://www.sentinelone.com/blog/sharepoint-toolshell-zero-day-exploited-in-the-wild-targets-enterprise-servers/
[20] https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a
[21] https://www.darktrace.com/blog/salty-much-darktraces-view-on-a-recent-salt-typhoon-intrusion



Origin

Based on assessments by trusted partners and reliable sources, the largest share of MAI that could be linked to a country in our ecosystem was associated with China-linked threat actors (37%), closely followed by Russia-linked threat actors (32%). Democratic People's Republic of Korea (North Korea) (11%) and the Islamic Republic of Iran (Iran) (7%) ranked third and fourth respectively. The remaining 13% was distributed across 10 other countries.

> Linking threat actors to geography remains a complex challenge. Our approach prioritises technical attribution by trusted partners and reputable sources to link activity to a country of origin, where feasible. False flag operations further complicate this exercise, as threat actors may deliberately project a misleading geographic origin.

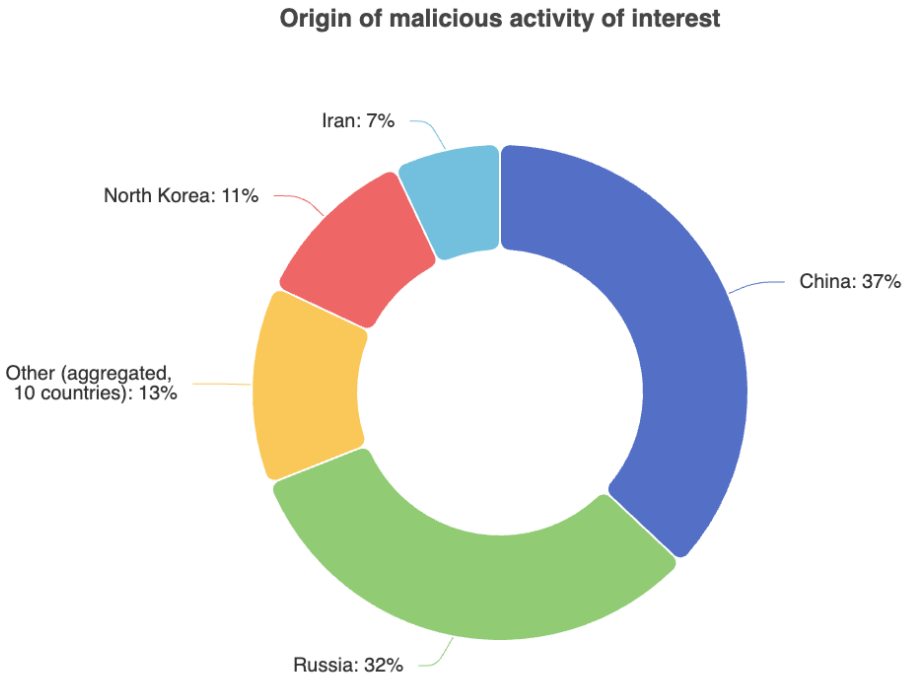
China-linked threat actors maintained a persistent presence in the EU threat landscape, primarily through **broad exploitation of vulnerabilities and supply-chain compromises**, often leveraging unpatched **edge devices** and third-party dependencies.[22]

Russia-linked threat actors remained consistent with patterns observed in previous years. Their primary focus was entities in Ukraine, followed by **entities in EU countries involved in support for Ukraine**.

North Korea-linked threat actors increasingly focused on European targets, notably through Operation DreamJob[23] and the IT Workers[24] scheme.

Iran-linked activity in Europe decreased compared to previous years, with threat actors likely redirecting efforts towards regional adversaries during the Iran-Israel escalation in June 2025.

[22] https://www.recordedfuture.com/research/rednovember-targets-government-defense-and-technology-organizations
[23] https://www.welivesecurity.com/en/eset-research/gotta-fly-lazarus-targets-uav-sector/
[24] https://therecord.media/north-korean-it-worker-scam-spreads-to-europe



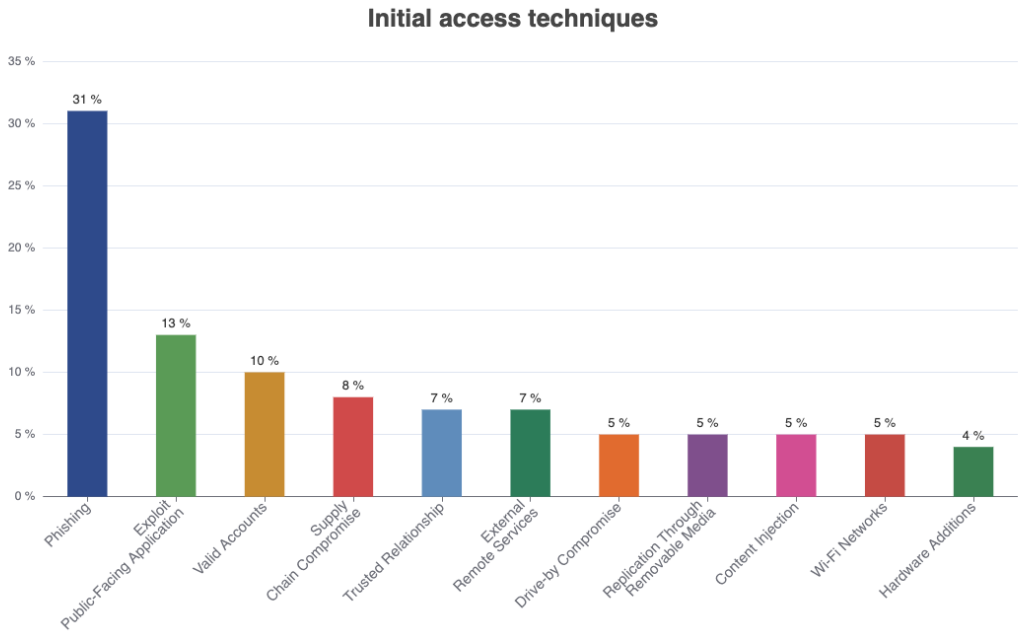
6 Tactics, techniques and procedures

We mapped the tactics, techniques, and procedures (TTPs) of MAI. Below we analyse the most notable TTPs observed in 2025.

Initial access techniques

The most frequently observed attempted initial access techniques were **phishing, exploitation of public-facing software, and valid account compromise**[25]. Despite its prevalence, phishing campaigns, especially e-mail phishing, did not seem to result in significant success given the number of attempts. However, there is a possible shift in trends toward voice phishing, which we discuss below.

[25] The use of stolen or legitimate credentials.



Significant incidents. Exploitation of **public-facing software** remained the initial access vector with the highest impact. In 2025, we dealt with nine significant incidents, **including one at a service provider** with access to a Union entity's internal systems. **Vulnerability exploitation was the initial access vector in seven of these incidents: two involved zero-day vulnerabilities, two targeted industrial control systems, two exploited stack-based buffer overflows, and one involved a firewall compromise.** In the remaining two cases, one intrusion came through the compromised service provider and the other's initial access technique could not be determined.

This represents a decrease from the 15 significant incidents recorded in 2024. The cause remains unclear, but **we do not interpret it as a reduction in threats or an indicator of improved defences.** We are currently unable to affirm the reason for this shift.

Vulnerability exploitation

As in 2024, the **exploitation of vulnerabilities in internet-facing devices remained the most impactful initial access method.** The most prominent software exploited in our ecosystem were Fortinet FortiGate[26], Ivanti Connect Secure devices[27], Ivanti Endpoint Manager Mobile devices[28], Citrix NetScaler[29], Microsoft SharePoint[30], Omnissa Workspace One[31], and React Server Components[32].

Credential theft, social engineering, and spoofing

Voice phishing as primary vector. In 2024, e-mail-based spearphishing encompassed 41% of initial access techniques. In 2025, this declined to 31%. 2025 saw a rise in voice phishing campaigns. This indicates an increase in human-targeted, non-digital social engineering channels.

For example, in June, UNC6040, a cybercrime actor, reportedly phoned employees of multiple service providers and, under the pretext of urgent IT checks, talked them into approving malicious OAuth connected apps inside

[26] https://arcticwolf.com/resources/blog/console-chaos-targets-fortinet-fortigate-firewalls/
[27] https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-exploiting-critical-ivanti-vulnerability?hl=en
[28] https://ccb.belgium.be/advisories/warning-actively-exploited-zero-day-vulnerabilities-ivanti-endpoint-manager-mobile-epmm
[29] https://www.rapid7.com/blog/post/etr-zero-day-exploitation-of-netscaler-adc-and-netscaler-gateway/
[30] https://www.microsoft.com/en-us/msrc/blog/2025/07/customer-guidance-for-sharepoint-vulnerability-cve-2025-53770/
[31] https://slcyber.io/research-center/secondary-context-path-traversal-in-omnissa-workspace-one-uem/
[32] https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components

Salesforce.[33] More than 90 organisations worldwide were affected, among them several vendors for Union entities.

Adversary-in-the-Middle (AiTM). AiTM attacks involve adversaries positioning themselves between a user and a legitimate service to intercept, manipulate, and hijack communication sessions. We observed several AiTM phishing attempts in our constituency, which in some cases led to successful compromises. Further, AiTM Phishing-as-a-Service kits were disseminated globally. In January, a new AiTM kit named Sneaky 2FA, targeted Microsoft 365 accounts by bypassing Multi-Factor Authentication (MFA).[34]

ClickFix browser prompts. ClickFix was a prominent and effective technique throughout 2025. Threat actors sought to trick users into executing malicious code by masquerading as routines to fix issues. We observed the mimicking of browser errors, the use of fake CAPTCHA overlays, the impersonation of Cloudflare Turnstile verifications, all to lure users into copying and running malicious PowerShell.[35]

Device-code authentication abuse. Adversaries lured victims into authorising device codes on legitimate sites, which were then captured, bypassing phishing filters and MFA. In February, multiple Russia-linked threat actors leveraged Microsoft's device-code flow to obtain tokens from users.[36]

Spoofed domains. We continued to observe attempts to impersonate Union entities online, including domain typosquatting, abuse of associated branding or logos, and website cloning.

Impersonation of individuals. In 2025, we continued to observe the impersonation of individuals, including high-ranking officials and politicians, in phishing campaigns and as fake accounts on social media platforms, such as LinkedIn, Facebook, Instagram, X, TikTok, and Signal.

Search Engine Optimisation (SEO) poisoning. Threat actors manipulated search results in trusted search engines to make malicious pages appear legitimate and show up higher in rankings. This leveraged the assumption that top hits are credible. For example, in September a global campaign used SEO poisoning to lure users to fake Ivanti VPN download sites to harvest VPN credentials.[37]

Use of infostealers

Cybercrime actors **widely used infostealer malware to harvest information from infected systems**, particularly data stored in web browsers such as credentials, authentication cookies, autofill information, and locally stored tokens. Stolen data was typically aggregated into infostealer logs and traded on criminal marketplaces. Infostealers were a key enabler within the cybercrime ecosystem, providing credentials and session tokens which facilitated downstream attacks.[38]

Supply-chain compromise

Despite a slight decrease in directly observed supply-chain compromises, this vector remained prevalent. Campaigns targeted both human and technical elements of software development. The majority of supply-chain attacks involved **poisoning open-source dependencies or source code**. For more information on observed targeted software, see section 10 (Software) below.

- In 2025, we observed **26 MAI relating to npm**, the standard package manager for Node.js. The high number for a single vendor likely reflects the continued vulnerability of open-source supply chains.
- In September, the self-replicating worm **Shai-Hulud** compromised more than 500 packages on the npmjs.com registry.[39] A November follow-up wave, Shai-Hulud 2.0, automated the same chain of credential

[33] https://cloud.google.com/blog/topics/threat-intelligence/voice-phishing-data-extortion
[34] https://blog.sekoia.io/sneaky-2fa-exposing-a-new-aitm-phishing-as-a-service/#h-url-patterns
[35] https://www.microsoft.com/en-us/security/blog/2025/08/21/think-before-you-clickfix-analyzing-the-clickfix-social-engineering-technique/
[36] https://www.volexity.com/blog/2025/02/13/multiple-russian-threat-actors-targeting-microsoft-device-code-authentication/
[37] https://www.zscaler.com/blogs/security-research/spoofed-ivanti-vpn-client-sites
[38] https://www.forbes.com/sites/daveywinder/2025/03/18/password-warning-as-21-billion-credentials-hit-by-infostealer-attacks/
[39] https://www.cisa.gov/news-events/alerts/2025/09/23/widespread-supply-chain-compromise-impacting-npm-ecosystem

theft and republished at higher speed, reflecting how a single stolen maintainer token can scale to many downstream code bases in a short period of time.[40]

Use of Operational Relay Box networks

Operational Relay Box (ORBs) networks are collections of compromised devices typically made up of vulnerable, often end-of-life SOHO routers, IP cameras, and VPS nodes. ORBs were typically used for conducting reconnaissance, scanning for, or exploiting vulnerabilities. In 2025, two new China-linked ORB networks were active in our ecosystem.

- **LapDogs**. This ORB consists of a slowly expanding constellation of around 1.000 primarily Linux-based SOHO routers and cameras, each back-doored with the self-signed-TLS implant ShortLeash.[41]
- **PolarEdge**. This ORB is a 2.000-node botnet delivered through CVE-2023-20118 to Asus, QNAP and Synology appliances. Its Mbed-TLS backdoor and PolarSSL-derived certificates overlap with the LapDogs ORB at the infrastructure layer.[42]

Cloud-based persistence and API abuse

Threat actors continued to exploit vulnerabilities in API security, misconfigured Identity and Access Management (IAM) policies, and exposed cloud secrets.

- **UNC6395 Salesforce campaign**. In August, UNC6395 harvested OAuth tokens for the Salesloft Drift plug-in to exfiltrate data from multiple corporate Salesforce tenants.
- **UNC6040 Salesforce campaign**. Threat actors leveraged legitimate platform features like Connected Apps and Data Loader, rather than exploiting vulnerabilities, shifting the attack surface to the authorisation model.[43]

Living-off-the-land techniques

Common Living-off-the-Land (LoL) techniques leveraged PowerShell, Windows Management Instrumentation (WMI), Remote Desktop Protocol (RDP), and various signed binary tools (LOLBin) on Windows and Linux. They allowed **threat actors to evade signature-based detection** and minimise forensic artefacts, effectively blending into normal system activity.

For example, in September, Russia-linked APT28's NotDoor campaign relied on built-in Windows tools like PowerShell and WMI to fetch and restart their code.[44]

Use of Artificial intelligence

Throughout 2025, threat actors sharpened their use of AI to generate phishing e-mails and malicious scripts, and to scale and automate their operations.

- **LLMs** continued to be leveraged in the automation, refinement, and scaling of cyberespionage campaigns. The observed use of LLMs to enhance voice phishing campaigns with voice cloning, personalised e-mail text, and deepfakes of officials and other high-profile individuals reflects this evolution. For example, in October 2025, a China-linked threat actor likely used LLMs in its spearphishing campaigns given the pacing, incoherent decision-making, and variety of the campaigns. The spearphishing e-mails used various themes and fictional identities, written in English, Chinese, Japanese, French, and German.[45]

[40] https://www.netskope.com/blog/shai-hulud-2-0-aggressive-automated-one-of-fastest-spreading-npm-supply-chain-attacks-ever-observed
[41] https://securityscorecard.com/wp-content/uploads/2025/06/LapDogs-STRIKE-Report-June-2025.pdf
[42] https://blog.sekoia.io/polaredge-unveiling-an-uncovered-iot-botnet/
[43] https://cloud.google.com/blog/topics/threat-intelligence/voice-phishing-data-extortion
[44] https://lab52.io/blog/analyzing-notdoor-inside-apt28s-expanding-arsenal/
[45] https://www.volexity.com/blog/2025/10/08/apt-meets-gpt-targeted-operations-with-untamed-llms/

- **Agentic AI.** A case in September 2025 illustrated one of the first publicly known cyberespionage campaigns that likely leveraged agentic AI. A reportedly China-linked threat actor directed a jailbroken, agentic AI system against 30 entities in the technology, finance, manufacturing and government sectors, achieving autonomous intrusion in a small number of cases. [43] This could indicate a rapid evolution as adversaries seek to scale and lower barriers to sophisticated intrusions.

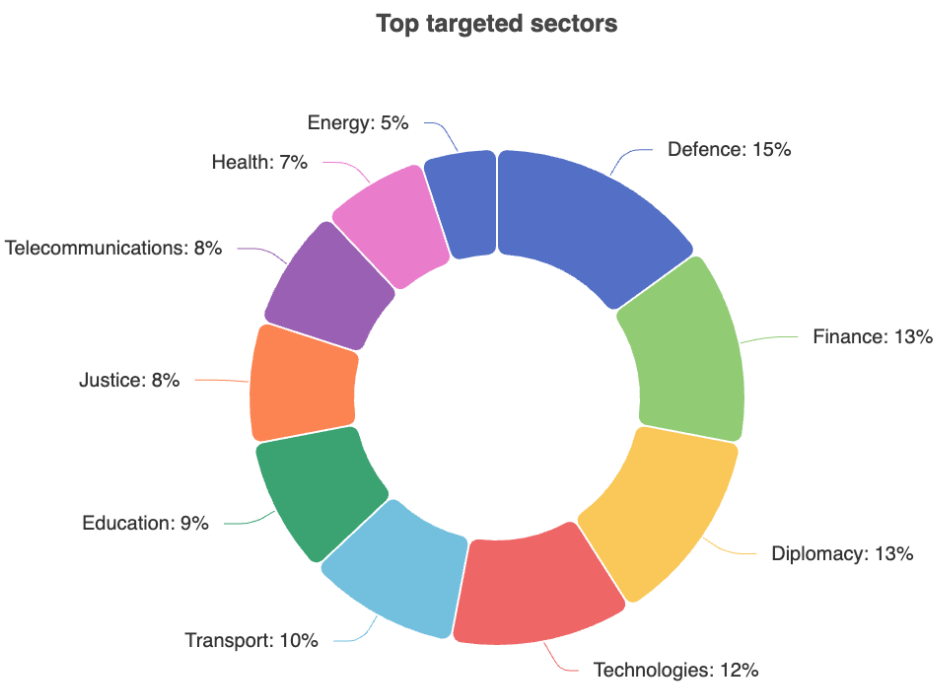
7 Sectors

We categorised MAI by sector, excluding public administration, in line with the taxonomy defined in our Cyber Threat Intelligence Framework.[46]

> The targeting of a particular entity within a sector does not necessarily indicate a deliberate focus on that sector by the threat actor. Such incidents may be opportunistic or coincidental.

The following assessment focuses on the five sectors with the highest attack frequency.

Successful intrusions into telecommunication providers were recorded[47], but not in sufficient volume to rank among the top five sectors discussed below. Nonetheless, intrusions into telecommunication providers carry significant downstream risk. For more information on the targeting of telecommunication providers, see Section 9 (Service providers) below.



[46] https://cert.europa.eu/publications/threat-intelligence/cyber-threat-intelligence-framework/
[47] https://www.darktrace.com/blog/salty-much-darktraces-view-on-a-recent-salt-typhoon-intrusion

Defence

The defence sector remained the most targeted sector in 2025. We observed **cyberattacks that appeared to be linked to ongoing conflicts**, including Russia's war on Ukraine and the Israel-Hamas conflict. Moreover, several state-sponsored cyberespionage campaigns targeted the sector. A few examples.

- In January, a Russia-linked cyberespionage actor conducted spearphishing campaigns that delivered malicious RDP files. The campaign used adversary-controlled domains that spoofed a defence manufacturer in an EU Member State.
- In October, North Korea-linked APT Lazarus Group reportedly used job offer lures to target private and public European defence firms, especially targeting entities involved with unmanned aerial vehicles (UAV).[48]
- In October, a Russia-linked cyberespionage actor reportedly created a fake domain referring to the International Defence Exhibition and Conference taking place in Slovenia.

Finance

The finance sector held a shared second place, along with the diplomacy sector. We processed more MAI, including more cybercrime, in 2025 than in 2024. **The finance sector was heavily targeted by cybercrime.** This explains why we recorded more attacks targeting finance overall.

The most frequent type of MAI targeting financial entities was data exposure & leaks by cybercrime groups followed by cyberespionage.[49] A few examples.

- In April, a cybercrime-linked scam impersonated the finance director of a Union entity.
- In December, a North Korea-linked actor reportedly used a Microsoft Teams-themed attack targeting the financial sector.
- In August, Iran-linked MuddyWater reportedly targeted financial executives worldwide, including in Europe.[50]

Diplomacy

The diplomatic sector, which includes Ministries of Foreign Affairs and embassies, was the second most targeted sector alongside finance, with cyberespionage as the primary threat. **Geopolitical events and meetings often triggered activity or were leveraged in campaigns.** A few examples.

- In January, Russia-linked APT29 reportedly impersonated a European Ministry of Foreign Affairs with fake wine tasting event invitations to install a stealthy modular backdoor.[51]
- The DoNot APT group reportedly conducted a spearphishing campaign targeting Southern European diplomatic entities by masquerading as officials and using diplomacy-themed lures.[52]

Technology

The technology sector was the fourth most targeted in 2025. Cybercrime actors continued to target this sector, with major threats including **data theft, data leaks, and ransomware**. Additionally, cyberespionage actors targeted technology companies in supply-chain attacks. A few examples.

[48] https://www.welivesecurity.com/en/eset-research/gotta-fly-lazarus-targets-uav-sector/
[49] https://www.threatfabric.com/blogs/sturnus-banking-trojan-bypassing-whatsapp-telegram-and-signal
[50] https://hunt.io/blog/apt-muddywater-deploys-multi-stage-phishing-to-target-cfos#Attribution_and_Overlaps
[51] https://research.checkpoint.com/2025/apt29-phishing-campaign/
[52] https://www.trellix.com/blogs/research/from-click-to-compromise-unveiling-the-sophisticated-attack-of-donot-apt-group-on-southern-european-government-entities/

- In May, intelligence agencies linked to 11 countries issued a joint cybersecurity advisory on a Russian cyberespionage campaign targeting US and European technology companies, especially those involved in aiding Ukraine.[53]
- In July, Semco Technologies, a French manufacturer of electrostatic chucks, was reportedly targeted by ransomware group Qilin, resulting in personal data being published on a dark web forum.[54]
- Throughout the year, the **npm** package registry was targeted with 26 supply-chain incidents. For more details, see Section 6 on TTPs.

Transport

The transport sector – encompassing air transport, maritime transport, and rail transport, which we aggregate for the purpose of this analysis – was targeted by cyberespionage campaigns, cybercrime groups, and supposed hacktivist groups. Notably, transport dropped from the second most targeted sector in 2024 to fifth in 2025. While **the sector remained equally targeted**, other sectors such as finance, diplomacy, and technology were more heavily targeted in 2025, causing the transport sector to rank lower. A few examples.

- An Iran-linked APT group reportedly conducted a spearphishing campaign targeting the aviation sector in Western European countries.
- In September, a reported ransomware incident at Collins Aerospace disrupted operations at multiple European airports for several days.
- In November, pro-Russia supposed hacktivists targeted the Danish transport sector with a DDoS campaign during Denmark's local elections.

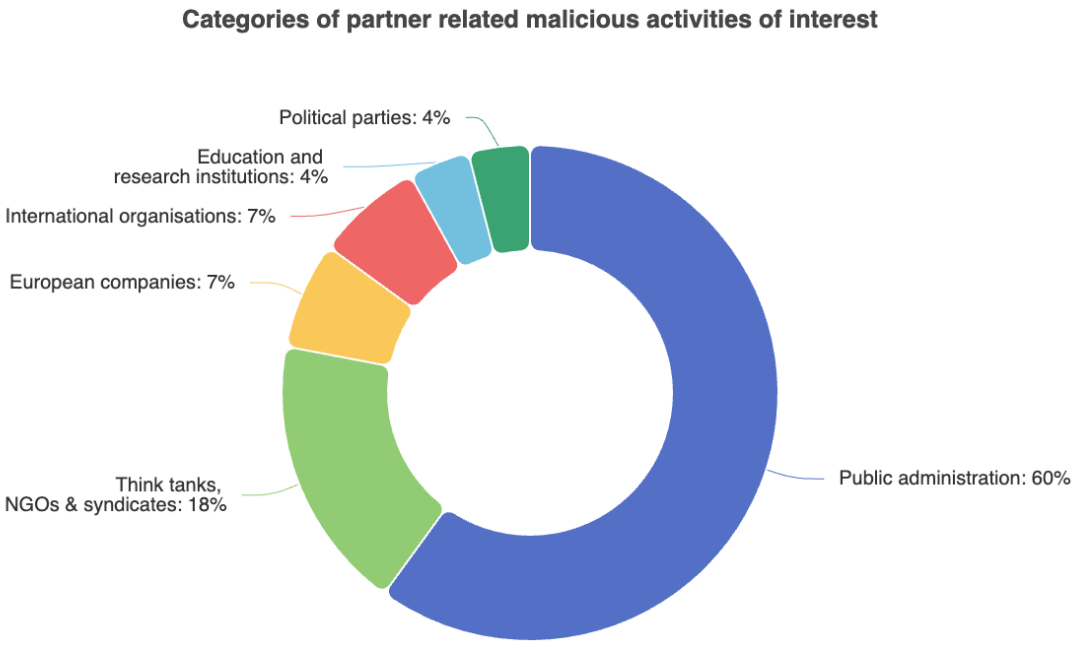
[53] https://media.defense.gov/2025/May/21/2003719846/-1/-1/0/CSA_RUSSIAN_GRU_TARGET_LOGISTICS.PDF
[54] https://www.latribune.fr/technos-medias/informatique/semi-conducteurs-semco-technologies-touchee-par-une-cyberattaque-de-hackers-russes-1029150.html

8 Partners

In 2025, we observed **178 cases of MAI targeting 90 organisations assessed to be partners of our constituency.** The targeted partner organisations were categorised into the following groups:

- Public administrations.
- Think tanks, NGOs & syndicates (such as trade unions).
- European companies.
- International organisations (such as the International Criminal Court and the European Space Agency).
- Education and research institutions.
- Political parties.

Public administrations accounted for 60% of partner-related malicious activity, followed by think tanks, NGOs and syndicates (18%), European companies and international organisations (both 7%), education and research institutions (4%), and political parties (4%).



MAI targeting partners typically involved to **spearphishing, data breaches, business e-mail compromises (BEC), DDoS, and ransomware.** A few examples follow.

- In March, the Polish government reported unauthorised access to the Polish Space Agency's IT infrastructure.[55]
- In June, the International Criminal Court disclosed that it had responded to a sophisticated cyber incident.[56]
- In July, the Dutch Public Prosecution Service went offline for several weeks, reportedly after a critical vulnerability was exploited in software used for remote access to its internal network[57].
- In November, four Danish political parties, with a presence in the European Parliament, were targeted with DDoS attacks by pro-Russia supposed hacktivists[58].
- In December, the French Ministry of Interior reported a data breach involving the Criminal Records Processing System and the Wanted Persons File.[59]

[55] https://www.reuters.com/world/europe/cyberattack-detected-polish-space-agency-minister-says-2025-03-02/
[56] https://www.reuters.com/technology/icc-says-new-cybersecurity-incident-has-been-contained-2025-06-30/
[57] https://nltimes.nl/2025/07/21/dutch-prosecution-service-faces-weeks-long-internet-outage-cyber-breach
[58] https://therecord.media/denmark-election-political-government-websites-ddos-incidents
[59] https://www.euronews.com/2025/12/17/french-interior-ministry-targeted-in-massive-cyberattack-minister-confirms

MAI targeting partners mostly impacted Union entities through increased **credential phishing** (originating from compromised partner e-mail accounts) and **data exposure** when partners suffered data breaches.

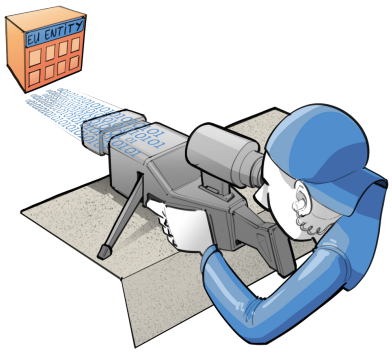
9 Service providers

In 2025, 32 service providers supporting our constituency experienced MAI. **In one case, the compromise of a service provider with access to a Union entity's internal systems led to a significant incident.** The case demonstrated the potential exposure created through trusted third-party access.

Successful intrusions into telecommunication providers were recurrent, though not widespread, and carry significant downstream risk. Reported incidents in the US serve as a warning to maintain heightened vigilance.[60] We assess the overall threat level as elevated, not due to the frequency of attacks, but because of the severity of potential consequences. We therefore maintain enhanced monitoring and analysis of all incidents involving telecommunications providers within our constituency.

Notable examples include the following.

- In July, Post Luxembourg reportedly experienced an unspecified cyberattack which resulted in outages but not in unauthorised access to data.[61]
- In July, as discussed in Section 5 (Threat Actors), **Salt Typhoon, a China-aligned threat actor reportedly compromised a European telecommunications provider by exploiting a vulnerability in Citrix NetScaler Gateway appliances**.
- In August, Colt Technology Services, a UK-based company involved in fibre connectivity reportedly experienced a Warlock ransomware attack, which disrupted the company's internal systems and resulted in data exfiltration.[62]
- In August, media sources reported that Bouygues Telecom, a French company, suffered a data breach which impacted 6,4 million customers, exposing IBANs and contractual details.[63]
- In August, media sources reported that Orange Belgium suffered a breach resulting in unauthorised access to 850.000 accounts.[64]
- In September, **a Union entity experienced a significant incident linked to a nation-state actor through a compromised service provider** that had been granted access to the Union entity's systems.
- In November, Proximus Belgium experienced a DDoS attack by pro-Russia supposed hacktivists which disrupted the website but did not cause unauthorised access to data.[65]

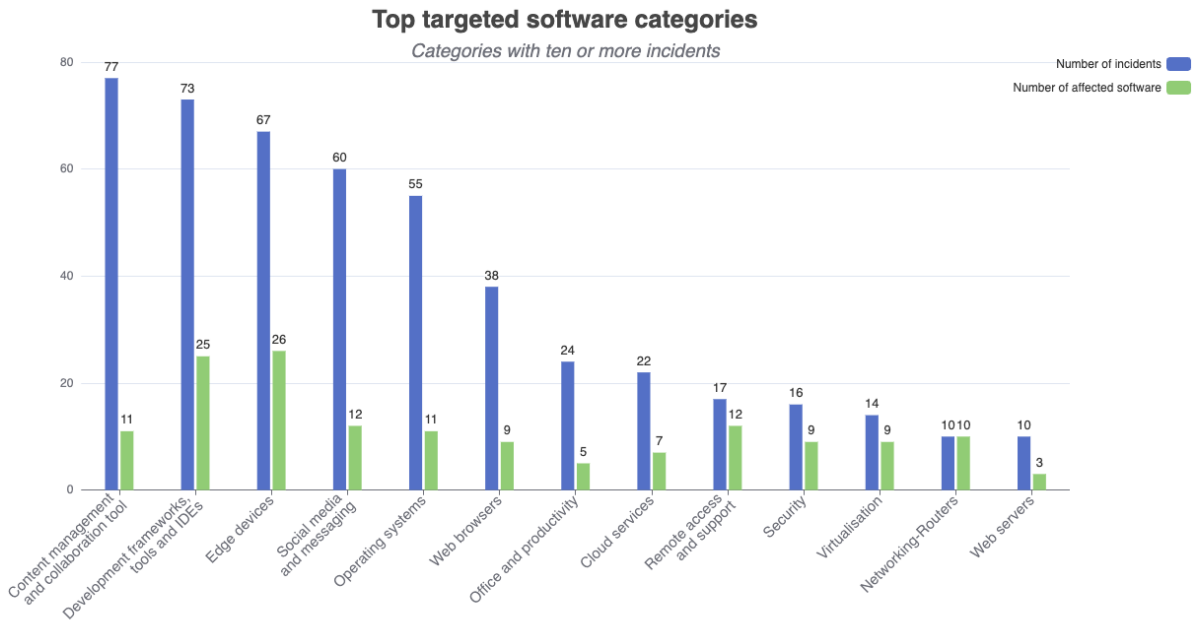


[60] https://www.securityweek.com/major-us-telecom-backbone-firm-hacked-by-nation-state-actors/
[61] https://chronicle.lu/category/telecomms/56053-cause-of-post-luxembourg-outage-identified-as-exceptionally-advanced-cyber-attack
[62] https://www.securityweek.com/telecom-firm-colt-confirms-data-breach-as-ransomware-group-auctions-files/
[63] https://therecord.media/bouygues-telecom-france-cyberattack-data-breach
[64] https://www.securityweek.com/orange-belgium-data-breach-impacts-850000-customers/
[65] https://www.vrt.be/vrtnws/nl/2025/11/05/cyberaanval-op-websites-proximus-en-scarlet/

10 Software

In 2025, we detected **MAI involving 198 software products used by our constituency**, up from 110 in 2024, an 80% increase.

Targeted software categories



Overall, attacks affected products across 26 software categories. The most targeted categories were the following.

Content management and collaboration tools. Collaboration platforms and e-mail systems had the highest incident volume, with 77 attacks analysed across 11 platforms. The attacks were concentrated on a few platforms, including SharePoint, Teams, Exchange, Webex, Jira, and WordPress.

Development frameworks. MAI involving development tooling saw a sharp increase compared to 2024. We identified 73 incidents across 25 products, such as Node, GitHub/GitLab, Jenkins, Docker Hub, PyPI, and VS Code. Supply-chain compromise such as compromised dependencies, malicious packages in npm and PyPI, and malicious IDE extensions accounted for the bulk of this activity, illustrating how a dispersed software landscape creates multiple entry points.

Vulnerability exploitation in edge devices. We observed 67 cases of MAI across 26 edge device products, with Fortinet, Ivanti, Cisco, and Palo Alto accounting for the bulk of these. In almost every case, the initial access came through vulnerability exploitation targeting VPN, firewall, and ADC firmware. See our Common Vulnerabilities and Exposures (CVE) table below for a list of noteworthy CVEs in our ecosystem in 2025.

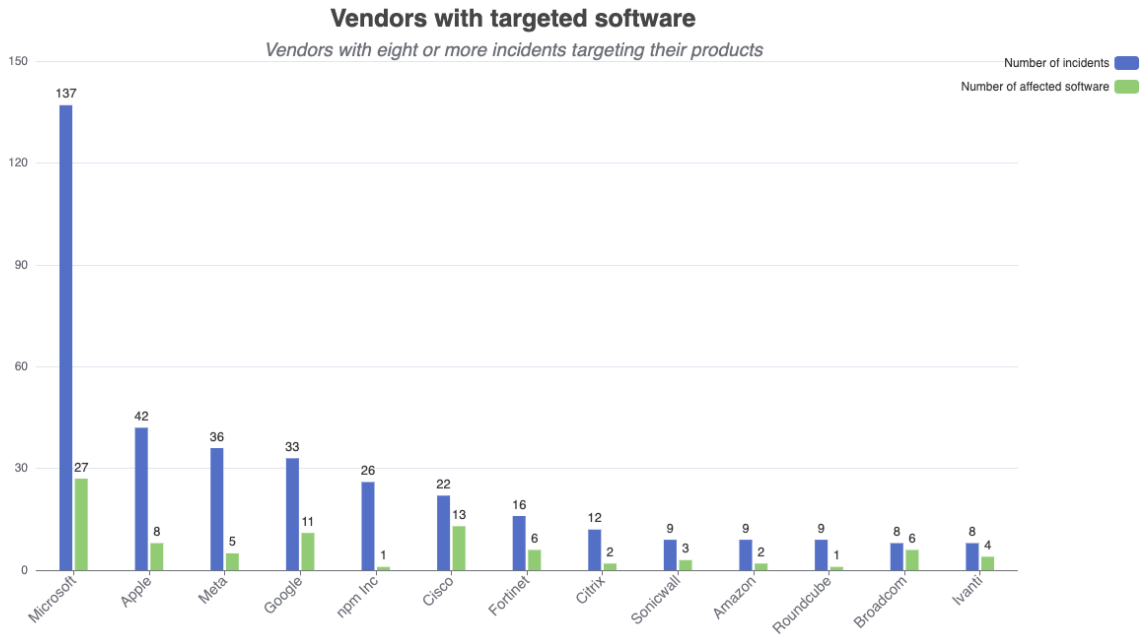
Social media and messaging apps. We observed 60 cases of MAI across 12 social media or messaging platforms, including LinkedIn, WhatsApp, Signal, and Zoom. This category reflects the growing use of voice and messaging platforms for social engineering, including OAuth abuse.

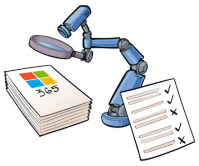
Operating systems. This category saw 55 incidents distributed across 11 products, such as iOS, tvOS, and macOS. Attacks included both classic server-side exploits and, in several cases, zero-day exploitation of mobile operating systems to gain persistent device control.

Web browsers. There had been 38 attacks across 9 products. Campaigns typically deployed information-stealing malware or malicious extensions that exfiltrated cookies, stored credentials, and other local data before moving laterally.

Vendors with targeted software

We also analysed vendors with eight or more incidents targeting their products in 2025. The chart below provides an overview of the vendors who were involved in eight or more MAI, showing the number of incidents and number of affected products for each.





At the vendor level, **Microsoft** products were by far the most targeted in our ecosystem, with 137 incidents across 27 products. This large lead over the next vendor reflects the breadth of the exposed Microsoft surface. **Apple** follows with 42 incidents across eight titles, almost all mobile or desktop OS builds. **Meta** properties (WhatsApp, Facebook, React, Instagram, PyTorch) drew 36 incidents across five products. **Google's** products, including Chrome, Android, Chromium, Gmail, Calendar, Drive, Meet and OAuth endpoints, produced 33 incidents.

The **npm** package registry was notably targeted with 26 supply-chain incidents. Network and security appliance vendors, including **Cisco**, **Fortinet**, **Citrix**, **SonicWall**, **Broadcom**, and **Ivanti**, collectively accounted for significant targeting, consistent with the continued exploitation of edge devices for initial access.

A notable outlier was **Roundcube**, in which one webmail package triggered nine incidents. These were driven in large part by CVE-2025-49113, a pre-authentication remote code execution vulnerability.[66]

Notable software exploitations

Below we list the most notable exploited vulnerabilities per vendor. The list is made up of **CVEs which were widely exploited in our ecosystem**, and which we assess reflect the 2025 threat landscape as seen from our standpoint.

[66] https://www.cve.org/CVERecord?id=CVE-2025-49113

Vendor	Product	Notable CVE
Fortinet	FortiOS, FortiVoice, FortiWeb, FortiProxy	CVE-2024-55591, CVE-2025-32756, CVE-2025-25257, CVE-2025-64446, CVE-2025-58034, CVE-2025-59718, CVE-2025-59719
Microsoft	Windows Server 2008, 2012, 2016, 2019, 2022, 2025; Windows 10, 11; Microsoft Outlook, Microsoft Office, Microsoft 365 for Enterprise, Microsoft SharePoint, Microsoft Windows Server	CVE-2024-49113, CVE-2024-21413, CVE-2025-49704, CVE-2025-49706, CVE-2025-59287
Apple	macOS, iOS, iPadOS, tvOS, VisionOS, Safari, Google Chrome on iOS	CVE-2025-24201, CVE-2025-31200, CVE-2025-31201, CVE-2025-43300, CVE-2025-43529, CVE-2025-14174
Ivanti	Ivanti Connect Secure, Ivanti Policy Secure, Ivanti Neurons for ZTA gateways Ivanti Cloud Service Appliance, Ivanti Endpoint Manager Mobile	CVE-2025-0282, CVE-2025-0283, CVE-2025-4427, CVE-2025-4428, CVE-2025-53770, CVE-2025-53771
Google	Chrome, Android OS	CVE-2025-2783, CVE-2025-6558, CVE-2025-13223, CVE-2025-48633, CVE-2025-48572
Cisco	Identity Services Engine, IOS, IOS XE	CVE-2025-20281, CVE-2025-20337, CVE-2025-20352
SonicWall	SonicOS, SonicWall VPN (SMA100)	CVE-2024-53704, CVE-2021-20035, CVE-2023-44221, CVE-2024-38475
Palo Alto	PAN-OS	CVE-2024-3393, CVE-2025-0108
Citrix NetScaler	ADC, Gateway	CVE-2025-6543, CVE-2025-5777
Meta	WhatsApp for iOS, WhatsApp Business for iOS, WhatsApp for Mac, React Server Components	CVE-2025-55177, CVE-2025-55182
Roundcube	Webmail	CVE-2025-49113
Oracle	Oracle WebLogic Server	CVE-2024-21182, CVE-2025-61757
CrushFTP	CrushFTP	CVE-2025-2825, CVE-2025-54309
SAP SE	NetWeaver	CVE-2025-31324
VMWare	VCF operations	CVE-2025-41244

11 Conclusion and recommendations

The 2025 threat landscape confirms that Union entities and their ecosystem face sustained and diversifying cyber threats. Cyberespionage & prepositioning remained the dominant motive, while cybercrime accounted for a growing share of observed activity. The exploitation of internet-facing systems continued to be the most impactful initial access vector, and threat actors increasingly targeted partners and service providers as indirect pathways to our constituents.

Strategic foresight: what the data suggests for 2026

1. **Social engineering is highly likely to expand to other delivery vectors.** Trends in voice phishing-to-OAuth chain, ClickFix, device code abuse, and messaging platform exploitation suggest threat actors are shifting to alternative channels beyond e-mail. We assess that voice calls, messaging apps, browser-based prompts, and QR code phishing are likely to grow as vectors.
2. **AI-enabled social engineering at scale.** Growing cases of voice phishing, enhanced by voice cloning, and LLM use in generating personalised spearphishing content, reflect how AI has made and will very likely continue to make social engineering significantly more scalable and convincing.
3. **Identity and authorisation systems are an increasingly important attack surface.** The growing prevalence of attacks that abuse legitimate authentication and authorisation flows suggests that adversaries are expanding their focus into identity infrastructure.
4. **Supply-chain attacks will likely deepen beyond code dependencies.** The open-source supply chain remains highly vulnerable. We assess that threat actors will likely target the SaaS integration ecosystem: not just code dependencies but API connections, marketplace extensions, and cross-platform OAuth grants.
5. **Destructive attacks may extend beyond the warring parties.** The Polish wiper incident represents a geographic expansion of destructive operations. As Russia's war on Ukraine and conflict in the Middle East continue, we assess the threshold for destructive attacks against EU-adjacent targets is likely to lower.

Recommendations

Based on our analysis, we recommend the following priority actions for our constituency.

1. **Prioritise patching of internet-facing systems and edge devices.** The exploitation of unpatched edge devices (firewalls, VPN appliances, network management solutions) remained the initial access vector with the highest impact in 2025, including in significant incidents affecting Union entities. **Timely remediation of vulnerabilities in internet-facing infrastructure should be treated as the single highest-priority defensive action.**
2. **Implement phishing-resistant multi-factor authentication**. Conventional MFA was repeatedly bypassed through Adversary-in-the-Middle attacks, OAuth abuse, and session token theft. Our constituents should transition to phishing-resistant methods such as FIDO2/WebAuthn or certificate-based authentication.
3. **Strengthen supply-chain governance across the software lifecycle.** Supply-chain attacks targeted development tools, open-source dependencies, and software platforms at scale. With CERT-EU's help, Union entities should vet and monitor third-party software components, enforce integrity checks on dependencies, and maintain inventories of open-source usage.
4. **Restrict and monitor OAuth and API access in cloud environments.** Threat actors exploited overly permissive OAuth application authorisations and API access to exfiltrate data and maintain persistent access. Our constituency should whitelist permitted connected applications, enforce least privilege for API access, and monitor for anomalous OAuth grants.
5. **Review and harden connectivity with partners.** Threat actors exploited trusted relationships as a beachhead to attempt to breach Union entities. The primary impact was credential phishing from compromised partner e-mail accounts and exposure of shared data. Our constituency should assess shared access levels, implement network segmentation for partner connections, and establish mutual incident notification protocols with CERT-EU's support.
6. **Assess security posture of service providers and adopt end-to-end encryption.** 32 service providers supporting Union entities experienced MAI in 2025. Telecommunications providers pose a heightened risk.

Our constituency should evaluate the security posture of service providers, ensure contractual incident notification obligations, develop contingency plans for provider compromise, and adopt end-to-end encryption as the default, at least for sensitive communications, to mitigate the risk of interception at the infrastructure level.

7. **Develop detection capabilities for social engineering beyond e-mail.** Threat actors increasingly used voice phishing, messaging platforms, fake error prompts (ClickFix), and impersonation of officials to bypass traditional e-mail-focused anti-phishing controls. With CERT-EU's help, Union entities should extend awareness training and detection capabilities to cover phone-based, messaging-based, and browser-based social engineering vectors.
8. **Monitor for impersonation and brand abuse across digital platforms.** Threat actors impersonated our constituency through lookalike domains, fake social media accounts, cloned websites, and misuse of the EU emblem. Union entities should leverage CERT-EU's proactive monitoring and takedown procedures for brand abuse.
9. **Maintain heightened vigilance during global events.** 44 distinct events were linked to malicious cyber activity in 2025. Threat actors used events as both lures for social engineering and triggers for reactive operations. Our constituency should anticipate increased threat activity around events relevant to their mandate, including enhanced monitoring during the event period with CERT-EU's support.
10. **Prepare for destructive attacks, particularly in critical infrastructure sectors.** While destructive attacks such as wipers remained rare outside direct conflict zones, the Sandworm-linked attempted wiper attack on a Polish renewable energy operator demonstrated that such attacks could reach EU territory. Union entities in energy and critical infrastructure sectors should ensure robust backup, recovery, and resilience capabilities.

CERT-EU continues to support our constituency through vulnerability scanning, real time alerting, incident response, and threat intelligence sharing. For further guidance on implementing these recommendations, our constituents are invited to contact us at services@cert.europa.eu.

While this report is primarily intended for Union entities, many of the threats, techniques, and recommendations described are relevant to organisations across all sectors. We encourage all readers to consider the findings in the context of their own cybersecurity posture. We welcome constructive feedback on this report at services@cert.europa.eu.

CERT-EU

THINK CONSTITUENT
CREATE VALUE

https://cert.europa.eu

services@cert.europa.eu

infosec.exchange/@cert_eu