
inetum.
Threat
Landscape
2025
Inetum LiveSOC

Index

1 Executive Summary 3

2 Context 5

3 Vitaminised LiveSOC 8

3.1 Evolution and improvement ____ 10

3.2 Operational management and coordination ____ 10

3.3 Activity balance ____ 11

4 Threat Analysis 15

4.1 Ransomware ____ 16

4.2 Advanced Persistant Threat ____ 17

4.3 DDoS ____ 19

4.4 Vulnerabilities ____ 21

5 Indicators of Compromise 23

6 Strategic Alliances 25

6.1 Partners and alliances ____ 26

6.2 National SOC Network (Spain) ____ 26

6.3 ICARO Project (Spain) ____ 26

6.4 FIRST (International) ____ 26

7 Deliverable products 27

8 2026 Trends 29

01

Executive Summary

Inetum is a multinational organisation whose core business is the provision of digital services. It has a strong presence in 19 countries: Belgium, Brazil, Bulgaria, Colombia, Spain, the United States, France, India, Ireland, Luxembourg, Morocco, Mexico, Peru, Poland, Portugal, the United Kingdom, Romania, Switzerland and Tunisia. In its commitment to cybersecurity and, specifically, defensive security, Inetum has a LiveSOC team, which aims to detect the most significant risks and threats to its customers at an early stage, managing a total of 154,601 alerts and 29,886 security incidents in 2025.

Throughout 2025, Inetum's LiveSOC **continues to grow with an intelligence-driven, adaptable and collaborative vision**, **fulfilling its mission to protect and strengthen its customers' digital resilience by anticipating and neutralising threats** using advanced detection techniques, artificial intelligence and automation.

The SOC, which currently has five locations (Madrid, Seville, Bilbao, Lisbon and Bogotá), is committed to geographical expansion, with particular emphasis on strategically strengthening the team in Colombia by providing support to guarantee 24/7 service, continuous support and an effective response to customer needs.

The Threat Landscape 2025 summarises the main findings of the work carried out by Inetum's LiveSOC throughout the year, offering an overview of the global threat landscape observed and highlighting some of the trends that will influence cybersecurity worldwide in 2026.

02
Context

During 2025, cyber-attacks linked to **physical conflicts** have continued to increase. Hybrid warfare, which was already a reality, now offers the **opportunity to launch combined attacks**. Armed conflicts have had a direct impact on the threat landscape, with the following being particularly relevant: Ukraine and Russia, tensions in the Middle East involving Israel, Iran and the United States, and the ongoing rivalry between India and Pakistan.

These scenarios have fuelled cyber campaigns aimed at sabotage, espionage and disinformation, carried out by **state-sponsored APT groups** (Advanced Persistent Threat) and directed against countries selected on the basis of geopolitical interests. Notable examples include APT29 (Russia) with campaigns against European diplomats and embassies, APT34 (Iran) against government entities, and APT41 and Mustang Panda (China) against critical sectors such as energy and manufacturing, among others.

Ransomware groups have maintained the upward trend in attacks already detected in 2024, with a total of 8,054 in 2025. Among the countries where Inetum has a presence, **Qilin, Akira, Cl0p, Play and INC Ransom** stand out as the most prolific groups. Furthermore, the top three countries attacked remain unchanged from 2024, led by the **United States, the United Kingdom and France.**

Distributed denial-of-service (DDoS) **attacks have reached historic levels**, with a 358% increase compared to 2024 and record peaks of 7.3 Tbps in just 45 seconds, according to Cloudflare records. CybelAngel has identified more than 300 threat actors involved in these campaigns, which have affected more than 100 countries. Considering only the countries where Inetum has a presence, France, the United States, India, Spain and Belgium are the ones that have been relatively most affected. Among the most active groups are NoName057(16), Keymous+, Dark Storm Team, Mr Hamza and RipperSec.

The number of vulnerabilities continues to grow, with 20% more being published in 2025 than in 2024. In the case of vulnerabilities with published exploits that a malicious actor could use as an attack vector, the percentages are similar in both years, corresponding to 19.94% for 2024 and 20% for 2025.

Phishing has remained one of the main attack vectors in 2025, using a wide variety of procedures, which actors are modifying and improving to increase their effectiveness. This year has seen a rise in campaigns using the Clickfix technique[1], QR code submissions, Quishing[2], with malicious .svg[3] images attached, and the use of OAuth spoofing to steal tokens and credentials[4].

Another notable trend has been the increase in attacks on the supply chain, especially in the **npm ecosystem**, where popular packages in development environments have been compromised. Carrying out massive malware attacks such as 'Shai-Hulud' for information exfiltration, as well as

[1] [Threat Report] Rise in Clickfix technique usage
[2] [Threat Report] Quishing campaign targeting VIPs
[3] [Threat Report] Active Phishing campaign with attached .svg files
[4] [Threat Report] Annual phishing report

campaigns to insert RATs into libraries with millions of downloads[5].

Currently, traditional cryptography based on algorithms such as RSA and ECC remains the cornerstone of digital security, but it faces a growing threat from advances in quantum computing. Although quantum systems capable of breaking these algorithms are not yet operational on a large scale, the 'harvest now, decrypt later'[6] strategy is already being employed by advanced actors, who collect encrypted information to decrypt it in the future. This scenario has prompted global initiatives. In the US, NIST[7] selected the first post-quantum algorithms for commercial and government use[8], while in Europe, ENISA has published guidelines recommending the transition to hybrid schemes (combining classical and post-quantum cryptography) as a temporary measure, and planning for complete migrations in critical infrastructures[9]. The European Commission, through the EU Coordinated Plan for Quantum-Safe Migration[10] of 2025, establishes specific deadlines for migration, with a strategic vision that seeks to anticipate the so-called Q-Day, the moment when quantum computing can break current algorithms.

Finally, the use of **artificial intelligence** in malicious campaigns has come to the fore.

State-sponsored groups, specifically from China, such as APT5 and APT15, have reportedly used ChatGPT to modify scripts, resolve configurations, and deploy malicious infrastructure[11]. Researchers at Anthropic published one of the most significant campaigns using AI in 2025, which allegedly used Claude to almost completely automate the Cyber Kill Chain[12], also attributed to a Chinese state actor, GTG-1002[13].

[5] [Advisory] NPM supply chain threat impacts CrowdStrike libraries, [Threat Report] Eslint-config-prettier malicious package campaign, [Threat Report] Supply chain attack on NPM packages, [NPM] Advisory - Critical 9.8 - React Native NPM package vulnerability

[6] Harvest Now, Decrypt Later (HNDL): The Quantum-Era Threat: https://www.paloaltonetworks.com/cyberpedia/harvest-now-decrypt-later-hndl

[7] NIST Releases First 3 Finalized Post-Quantum Encryption Standards: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[8] NIST Unveils Post-Quantum Cryptography (PQC) Standards: https://postquantum.com/quantum-policy/nist-pqc-standards/

[9] EUCC Guidelines on Cryptography: https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en

[10] Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography: https://eur-lex.europa.eu/eli/reco/2024/1101/oj/eng

[11] [Threat Report] The Weaponization of AI Emerging Attacks and Offensive Uses

[12] *Developed by Lockheed Martin, the Cyber Kill Chain® framework is part of the Intelligence-Driven Defence® model for identifying and preventing cyber intrusion activity. The model identifies what adversaries must complete to achieve their objective.* https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[13] Report: https://www.anthropic.com/news/disrupting-AI-espionage

03

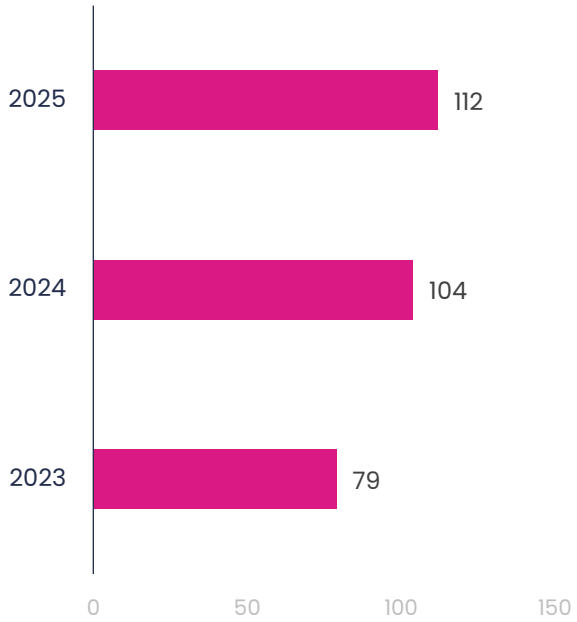
Vitaminised LiveSOC

In 2025, Inetum's LiveSOC has continued to grow with a **vision based on intelligence, adaptability and collaboration**, fulfilling its **mission to protect and strengthen the digital resilience of organisations by anticipating and neutralising threats** using advanced detection techniques, artificial intelligence and automation.

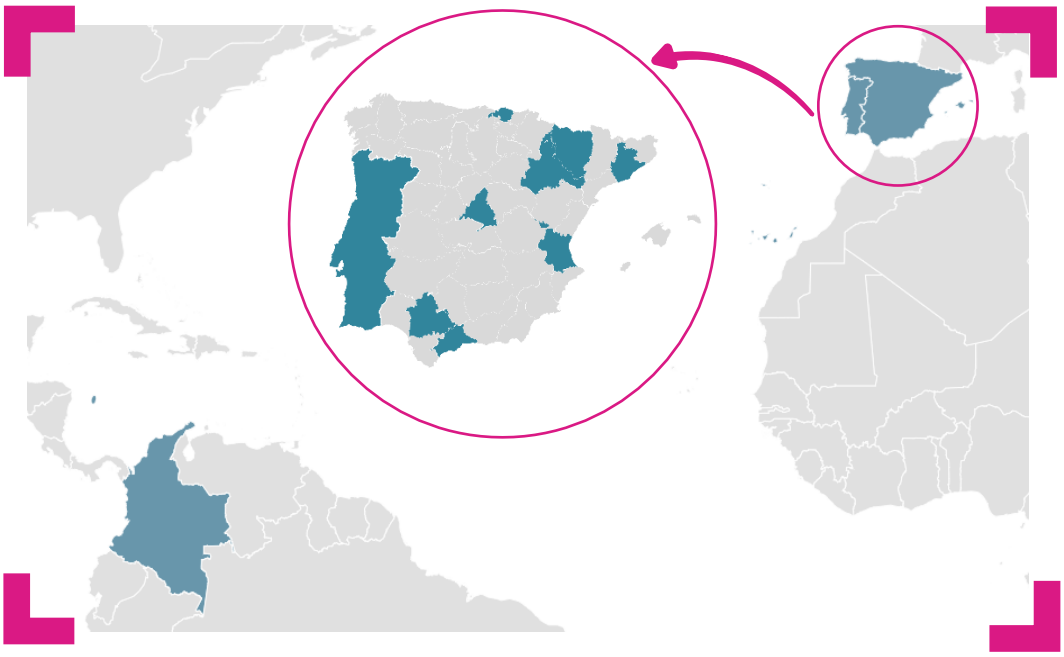
Following a strategic planning process, LiveSOC has evolved into an AI-powered model to optimise alert detection and analysis. To achieve this, it has incorporated automation and contextualisation through a workflow orchestration and automation platform used in state-of-the-art SOC environments. These advances have strengthened alert triage, providing additional information for assessment by the Incident Response analyst team. In addition, more in-depth actions have been deployed for the maintenance and standardisation of security incidents in accordance with CCN CERT, thus ensuring consistency in metrics and analysis and reinforcing both operational efficiency and service quality.

From the five SOC locations (Madrid, Seville, Bilbao, Lisbon and Bogotá) and with a staff distribution model that encompasses various Inetum sites in Spain, the company is committed to geographical expansion, strategically strengthening its team in Colombia in order to guarantee 24/7 service, continuous support and an effective response to customer needs.

Number of employees at Inetum's LiveSOC in 2023, 2024 and 2025



Geographical distribution of Inetum's LiveSOC staff in 2025



2.1 Evolution and improvement

During the first half of 2025 Inetum's LiveSOC implemented an automation layer based on a flow orchestration platform widely used in state-of-the-art SOC environments, capable of centralising and standardising alerts from multiple sources (EDR/XDR, SIEM, firewalls, antispam and open source intelligence).

This architecture has been integrated with artificial intelligence agents and threat intelligence sources to improve the quality of analysis and reduce triage times. These measures have made it possible to identify false positives more quickly, enrich alerts with contextual information, and automatically prioritise incidents in the ticketing system.

At the same time, these improvements have been observed in key indicator metrics, such as MTTR (Mean Time to Resolve)[14], which, under SLA[15] compliance criteria, has maintained a positive trend with values close to 100%.

2.2 Operational management and coordination

In terms of management, Inetum's LiveSOC has continued to improve the **standardisation of security incident categories**, with the aim of providing greater consistency in the classification and management of alerts. Taking as a reference the National Guide for the Notification and Management of Cyber Incidents, approved by the Spanish Government's National Cybersecurity Council, and the 'CCN-STIC 817 on Incident Management' guide from the National Cryptology Centre (CCN-CERT), within the framework of the National Security Scheme.

[14] MTTR reflects the percentage of alerts managed within the committed timeframes, serving as an indicator of efficiency and operational quality.

[15] A service level agreement (SLA) is a contract between a service provider and a customer that defines the service to be provided and the level of performance to be expected. An SLA also describes how performance will be measured and approved, and what happens if performance levels are not met. https://www.ibm.com/mx-es/think/topics/service-level-agreement.

This standardisation allows for the establishment of a clear categorisation that distinguishes between different incident taxonomies, standardising the nomenclatures used by different security technology providers. As a result, the quality of the information collected is improved, facilitating a more agile, accurate and coordinated response.

At the same time, collaboration between the CSIRT and Threat Intelligence teams has been strengthened, improving the early identification of active campaigns and supporting the analysis of complex incidents. This coordination has facilitated the detection of relevant indicators of compromise and their rapid dissemination, contributing to the strengthening of the preventive capabilities of customer systems and the anticipation of possible attack vectors. This collaboration, based on the TaHiTI[16] methodology, articulates the tactical integration between intelligence and threat hunting, enabling advanced correlation of indicators, early detection and execution of proactive responses to emerging threats.

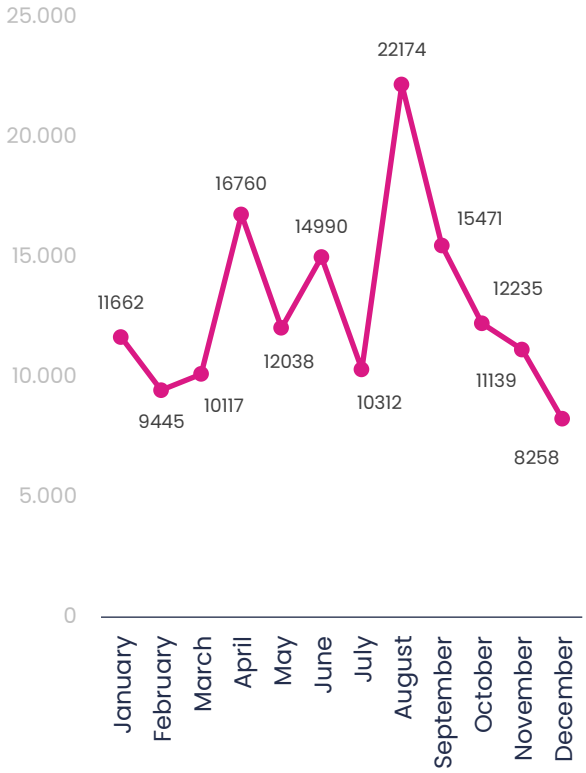
In addition, the Log Management team has worked throughout 2025 on continuously improving its multi-platform use case library, which streamlines deployments in different solutions with a high level of effectiveness, anticipating early monitoring and adding value from practically the moment a new service is taken on.

2.3 Activity balance

Incident Response

In 2025, the LiveSOC team detected and analysed 154,601 alerts[17] in total, managing 29,886 security incidents[18]. The distribution of the total number of alerts analysed throughout the year reveals a higher concentration in August, April, and September. In addition to the distribution based on criticality, the number of medium-level alerts was higher, followed by high-level alerts.

Security alerts per month in 2025

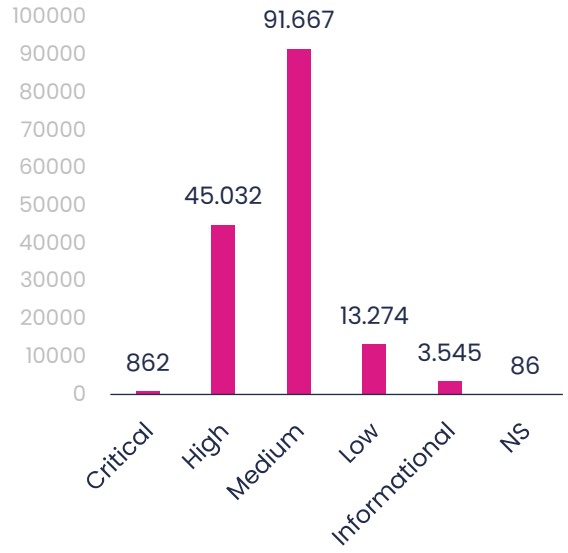


[16] Targeted Hunting integrating Threat Intelligence

[17] *Security alert: automatic notification generated by a security system (such as a SIEM, IDS, antivirus, etc.) indicating potentially suspicious or malicious activity.*

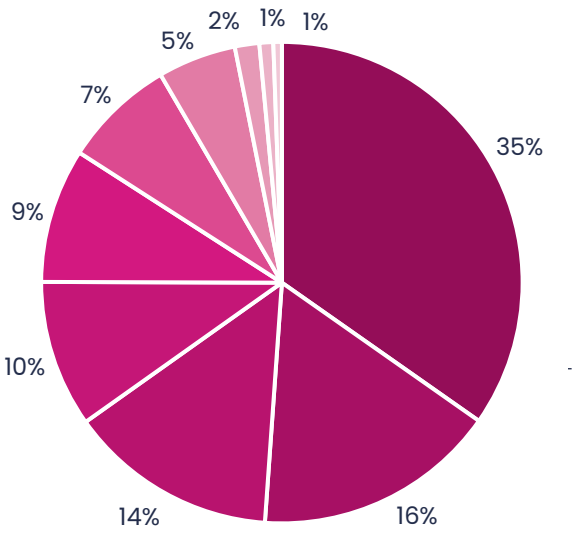
[18] *Security incident: An alert that has been analysed and confirmed as a real threat or security breach.*

Number of security alerts by criticality 2025



Of the 29,886 total security incidents managed, the following types stand out in terms of quantity: Malicious code, intrusion, confidentiality, fraud and intrusion attempt. Compared to 2024, there has been a considerable increase in the number of incidents in the following categories: Malicious Code (+197%), Intrusion (+82%) and Confidentiality (+64%). These categories continue to be the most frequently managed types of incidents for another year.

Percentage of security incidents by taxonomy 2025



Malicious Code

Malicious code encompasses **any software designed to disrupt the normal functioning of systems, networks or applications for harmful purposes**. It includes viruses, worms, Trojans, ransomware, spyware and malicious scripts. Its main objective is usually to steal information, encrypt data for extortion, interrupt services or allow unauthorised access, compromising the integrity and availability of systems.

Intrusion

Intrusions are **unauthorised accesses to systems, networks or applications**, usually through the exploitation of vulnerabilities or

compromised credentials. This type of incident can involve privilege escalation, backdoor installation or data manipulation, affecting the integrity and availability of the technological infrastructure.

Confidentiality

Confidentiality incidents occur **when sensitive information is accessed, disclosed, or exfiltrated without authorisation**. This includes data breaches, credential theft, and exposure of classified documents. This type of incident compromises privacy and can have critical consequences in government, corporate, or financial environments, affecting trust and regulatory compliance.

Fraud

Fraud consists of **actions aimed at deceiving or manipulating in order to obtain illicit benefits**, usually through techniques such as phishing, spear phishing, identity theft or financial fraud. These attacks seek to exploit the trust of users or systems to steal information, carry out fraudulent transactions or compromise financial resources, generating losses and damaging reputations.

Intrusion Attempt

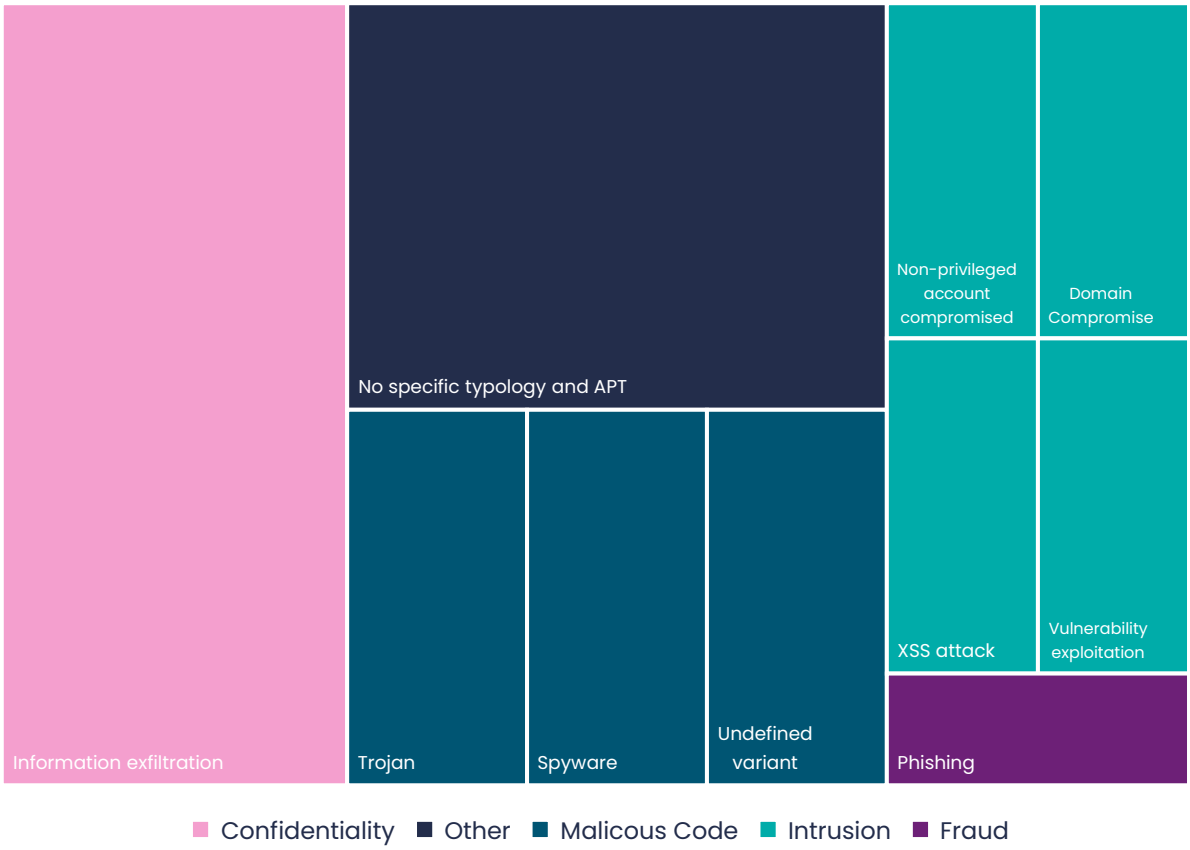
Intrusion attempts are detected **hostile activities that seek to compromise systems or networks**, even if they do not result in successful access. They include unauthorised login attempts and exploitation tests, among others. Although they may not have an immediate impact, they can be early indicators of an attack and require monitoring and response to prevent actual intrusions.

During the management of these incidents, the Incident Response Team has carried out **over 18,000 initial response actions**, including revoking sessions, resetting passwords, terminating processes, blocking domains and isolating hosts, to name a few. This shows that the service not only detects incidents early, but also proactively responds by deploying countermeasures to prevent incidents from evolving and amplifying.

CSIRT

By 2025, the CSIRT (Computer Security Incident Response Team) has established itself as a fundamental part of Inetum's LiveSOC, providing specialised capabilities for managing and responding to critical incidents, as well as complementing real-time monitoring and detection. In addition to collaborating on incident containment, eradication and recovery, it carries out forensic analysis and threat hunting. During this year, the CSIRT team has participated in the response to 179 incidents involving seven different clients. The incidents analysed by the team with the highest representation by taxonomy have affected:

Security incidents by number according to taxonomy managed by CSIRT 2025



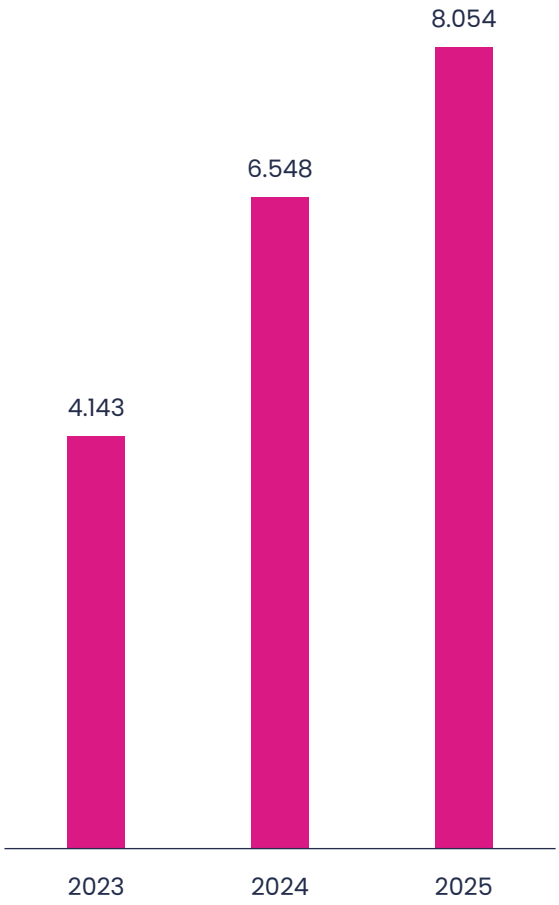
04

Threat Analysis

3.1 Ransomware

Ransomware has continued its upward trend since 2023, with a considerable increase in attacks in 2024 (6,548) and continuing throughout 2025 (8,054), making it one of the most significant threats in terms of both volume and impact on organisations.

Number of ransomware attacks per year in 2023, 2024 and 2025

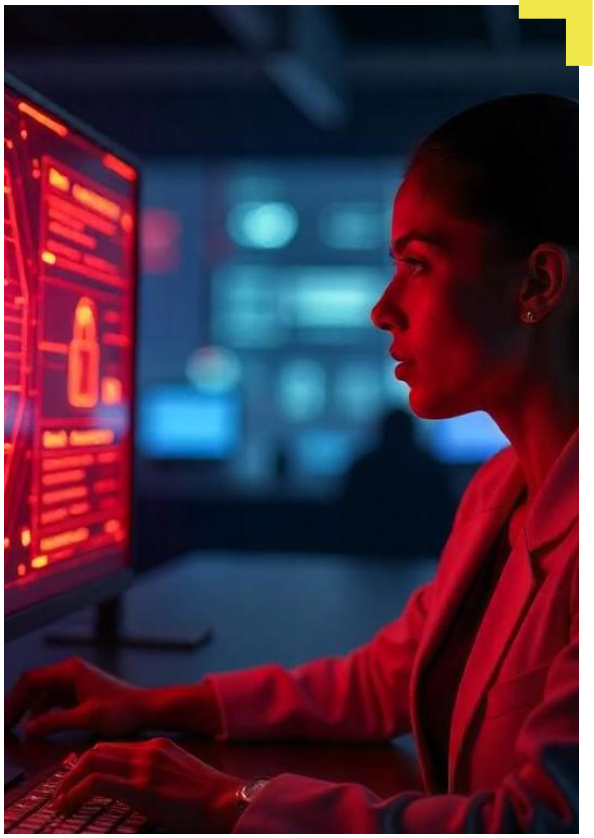


This year, the most prolific ransomware groups were **Qilin, Akira, Cl0p, Play and INC Ransom**, which attacked all 19 countries where Inetum operates. In terms of the ranking of these countries in terms of impact in 2024, the top three remain unchanged, with Spain, Mexico and Colombia climbing the rankings.

Top 10 countries targeted by ransomware in 2025

Top 10 Victim Countries 2025

=	United States
=	United Kingdom
=	France
+2	Spain
=	Brazil
-2	India
+2	Mexico
=	Switzerland
+5	Colombia
-3	Belgium



In line with these trends, the Threat Intelligence team has developed the following profiles of malicious actors in 2025[19]:

3.2 Advanced Persistant Threat

Advanced Persistent Threat (APT) **groups** continue to pose a critical risk to organisations and governments. These attacks, usually state-sponsored, are characterised by their sophistication, persistence and strategic focus, with objectives ranging from espionage and theft of sensitive information to sabotage and disinformation.

The activity of these actors reflects a clear correlation between geopolitical tensions and operations in cyberspace, mainly affecting critical infrastructure and sectors such as energy, telecommunications, defence and technology. In this context, campaigns attributed to actors linked to **Russia, China, North Korea and Iran** stand out. Along these lines, during 2025, the Threat Intelligence team has developed the following profiles of threat actors[20]:

[19] [Threat Actor Profile] Akira Ransomware, [Threat Actor Profile] Cl0p Ransomware, [Threat Actor Profile] FOG Ransomware, [Threat Actor Profile] Lynx Ransomware, [Threat Actor Profile] Medusa Ransomware, [Threat Actor Profile] Nova Ransomware, [Threat Actor Profile] Qilin Ransomware, [Threat Actor Profile] SafePay Ransomware, [Threat Actor Profile] DragonForce Ransomware, [Threat Actor Profile] Play Ransomware and [Threat Actor Profile] INC Ransom

[20] [Threat Actor Profile] APT29, [Threat Actor Profile] APT34, [Threat Actor Profile] Lazarus Group, [Threat Actor Profile] APT41 and [Threat Actor Profile] Mustang Panda

APT29

APT29, also known as Cozy Bear or The Dukes, is a **cyber espionage actor linked to Russian intelligence.** Active since at least 2014, this group has carried out intrusions in key sectors such as government institutions, healthcare, education, finance, telecommunications, energy and defence. Its presence has been detected in various regions around the world, including North America, Europe, Asia, Africa, and South America, demonstrating its global operational capabilities. Recognised for its advanced capabilities, APT29 employs a variety of sophisticated techniques, including cryptographic methods, stealth mechanisms, and custom malware such as MiniDuke, CosmicDuke, and OnionDuke.

APT34

The advanced persistent threat group APT34, also known as Oilrig, Earth Simnava or Helix Kitten, is believed to have begun operations in 2016 and its main objective is cyber espionage. In the current context of conflict in the Middle East, this actor could increase its importance with attacks against Israel or its allies. Since 2018, the US National Counterintelligence and Security Centre (NCSC) has considered the group **to be of Iranian origin, linked to entities such as the Iranian Ministry of Intelligence and Security (MOIS).**

Although its operations are mainly concentrated in the Middle East, APT34 maintains a global presence. It has remained active during the first half of 2025, and the activity detected could be related to the Iran-Israel and US military conflict of previous months.

Lazarus Group

The Lazarus Group, an APT backed by **North Korea**, has shown a steady increase in operational activity throughout 2025, particularly in late August and during the first half of September. Current campaigns have affected more than 36,000 victims worldwide, with an increase in campaigns targeting developers in Europe, India, and Brazil. Lazarus focuses on the modern software development lifecycle by implementing backdoors in cloned repositories, contaminating open-source package ecosystems, and exploiting container images and CI/CD touchpoints to deliver its payloads. Social engineering remains the primary tactic used by this group, which impersonates IT contractors and recruiters and conducts technical interviews with malware to place its loaders.

APT41

APT41, also known as Double Dragon, is a **sophisticated and prolific Chinese threat actor engaged in both espionage and financially motivated cybercrime**. Active since at least 2012, APT41 has targeted sectors around the world, including healthcare, telecommunications, finance, and government institutions.

The group is known for its advanced tactics, rapid operations, and ability to exploit vulnerabilities across various sectors.

The group has demonstrated remarkable adaptability, leveraging a broad toolset that includes custom malware, supply chain attacks, and zero-day exploits.

Mustang Panda

Mustang Panda is **a Chinese-sponsored cyber espionage threat group that has been active since at least 2014**. Over the years, it has launched numerous campaigns, with a notable increase in activity from 2023 to the present. These operations have mainly targeted countries in Asia, often coinciding with periods of political tension or diplomatic events.

The group focuses on gathering information, attacking government institutions, NGOs, religious organisations, and research centres. In 2024 and 2025, Mustang Panda significantly expanded its operations, shifting its geographical and strategic focus and impacting a wide range of countries and critical sectors, particularly in Europe.

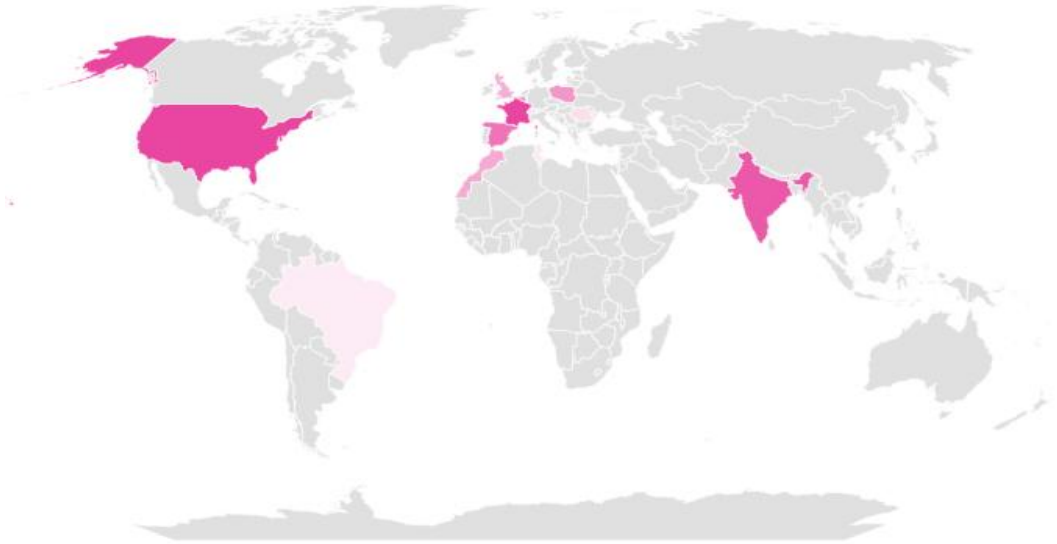
3.3 DDoS

Distributed Denial of Service (DDoS) attacks in 2025 have reached historic levels, becoming one of the most disruptive threats[21]. According to Cloudflare, 20.5 million attacks were mitigated in the first quarter alone, an increase of 358% over the previous year[22]. The all-time record was set in June, when it contained the largest DDoS attack in history: 7.3 terabits per second in just 45 seconds, equivalent to more than 37 terabytes of data launched against a hosting provider[23].

According to data from CybelAngel, these attacks have affected more than 100 countries, showing a wide distribution that is sometimes combined, affecting several regions at the same time. In 2025, more than 15,000 DDoS attacks were carried out, with 4,456 detected in countries where Inetum has a presence, with **France, the United States, India, Spain and Belgium** being the most attacked.

[21] [Threat Report] DDoS Campaign Proliferation, Vectors and Actors Involved
[22] Cloudflare Q1 2025: https://blog.cloudflare.com/ddos-threat-report-for-2025-q1/
[23] Cloudflare report on the largest DDoS attack of 2025: https://blog.cloudflare.com/defending-the-internet-how-cloudflare-blocked-a-monumental-7-3-tbps-ddos/

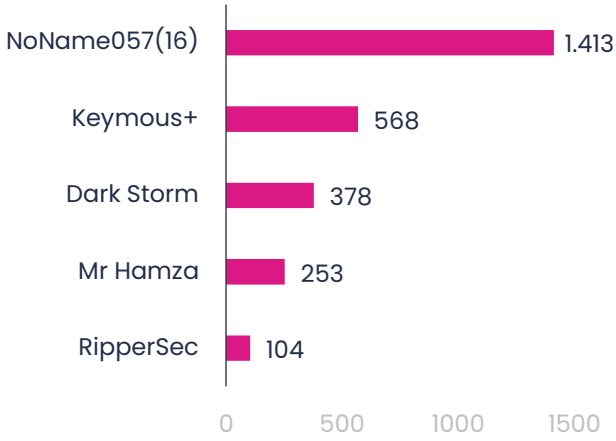
Geographical distribution of impact in countries where Inetum operates 2025



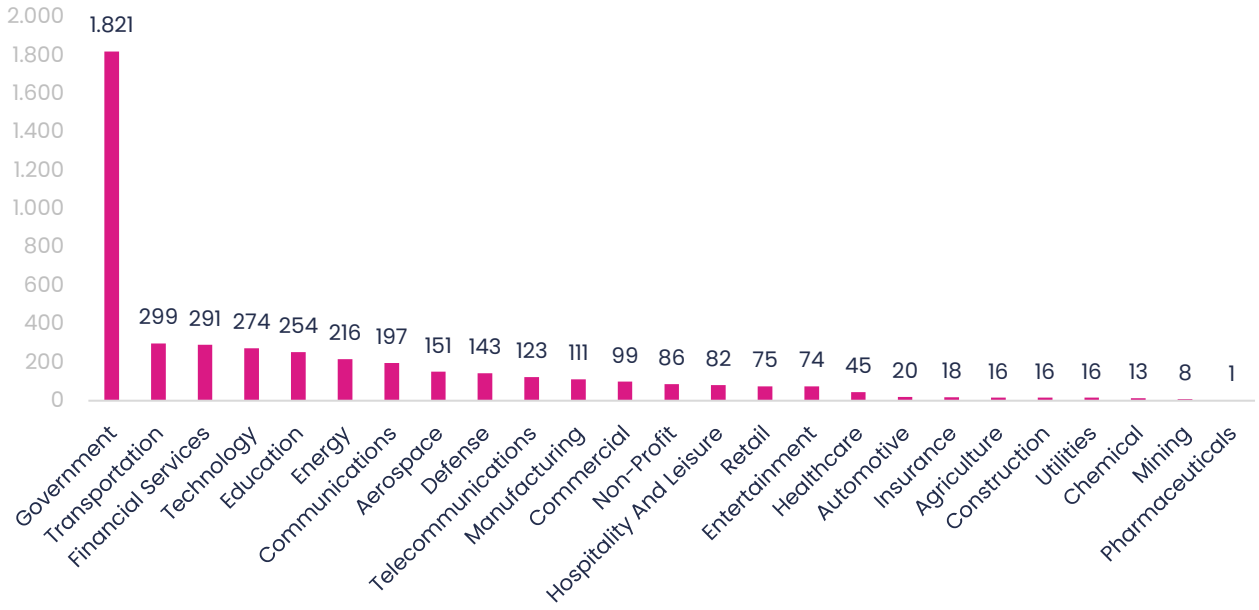
The impact of these attacks varies, but they have mainly affected the **government, transport, financial, technology and education sectors**.

These types of attacks have been used by more than 300 different threat actors, 195 of whom have orchestrated them against countries where Inetum has a presence. The most active ones include: NoName057(16), Keymous+, Dark Storm Team, Mr Hamza and RipperSec.

Top 5 DDOS actors in 2025



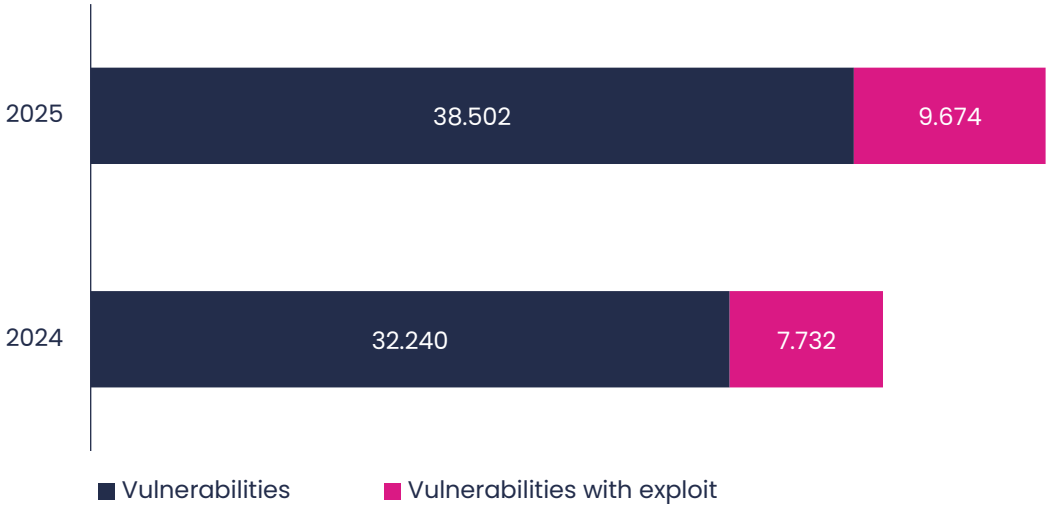
Distribution of attacks by sector 2025

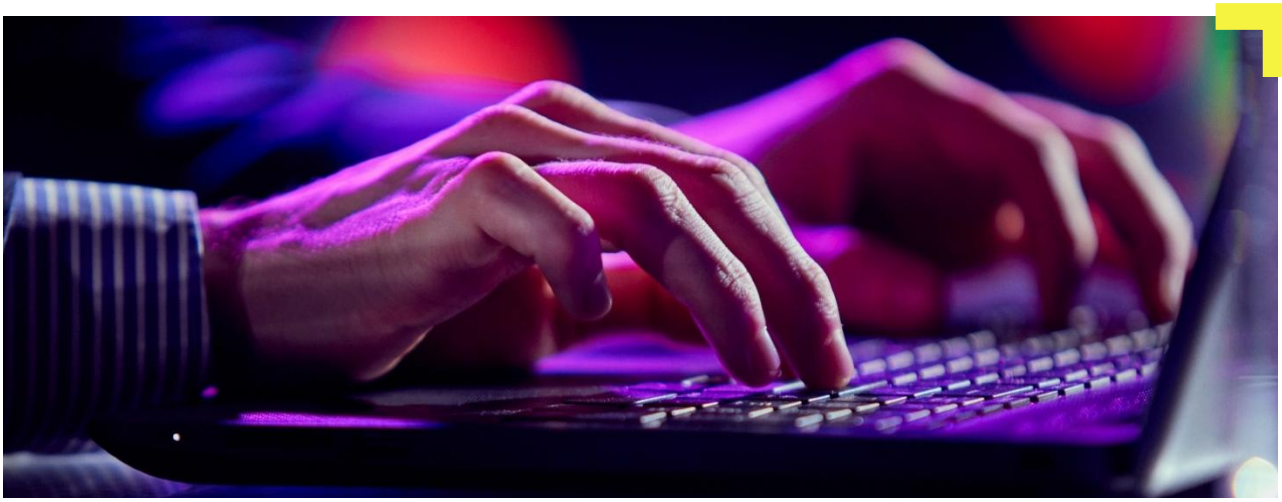


3.4 Vulnerabilities

In 2025, the number of vulnerabilities published increased by 20% compared to the previous year, according to the US National Institute of Standards and Technology (NIST). The percentages for vulnerabilities with associated exploits are similar in both years: 19.94% in 2024 and 20% in 2025.

Number of vulnerabilities published and vulnerabilities published with exploits 2024 and 2025

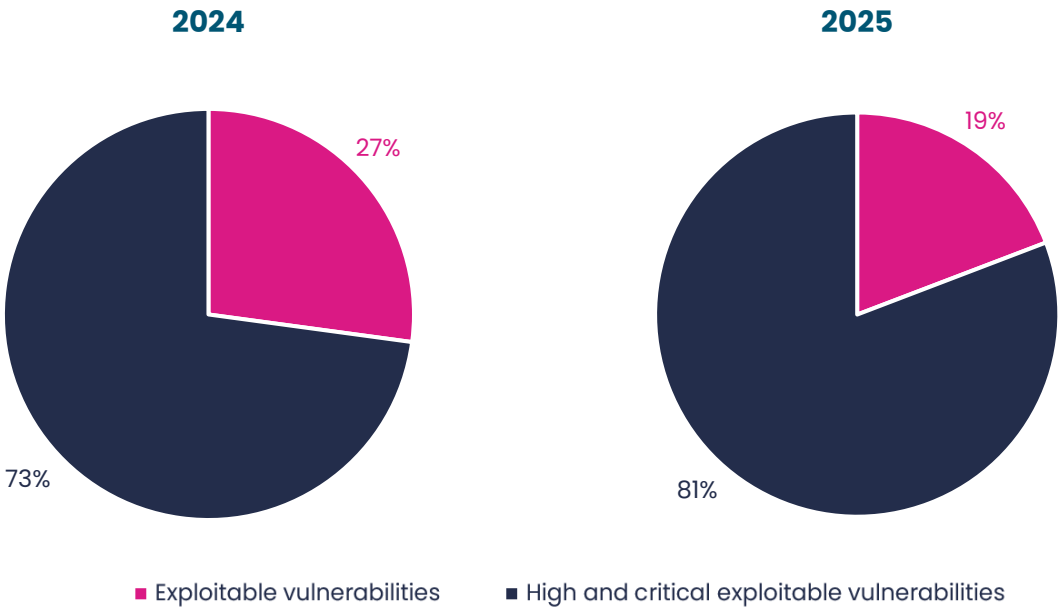




It is worth mentioning that, of the total number of vulnerabilities published with associated exploits, there has been a significant increase in the number of high- and critical-level vulnerabilities (scoring 7–10 on the CVSS[24] scale). There has been a 50% increase in this type of vulnerability in 2025 compared to 2024.

The Threat Intelligence team disseminates reports on the publication of vulnerabilities of a high and critical severity in order to alert Inetum LiveSOC customers to their existence and promote their remediation, achieving a 38% increase in vulnerability sharing in 2025 compared to 2024.

Percentages of high and critical vulnerabilities published with/without exploits, 2024 and 2025



Number of vulnerabilities shared by Threat Intelligence team in 2024 and 2025

[24] *Common Vulnerability Scoring System*

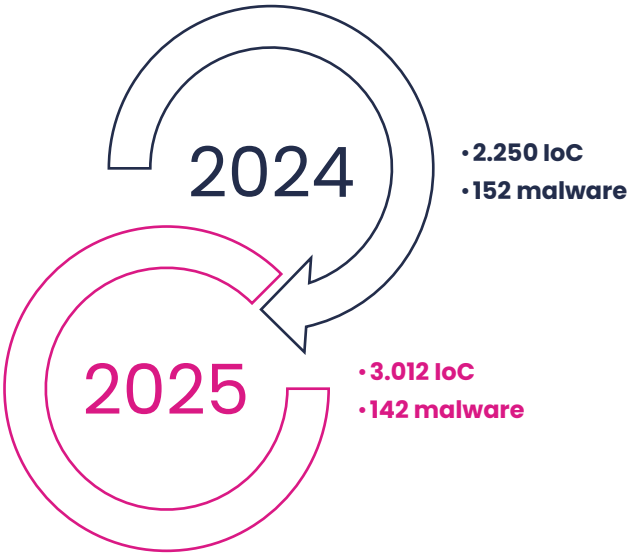
05

Indicators of Compromise

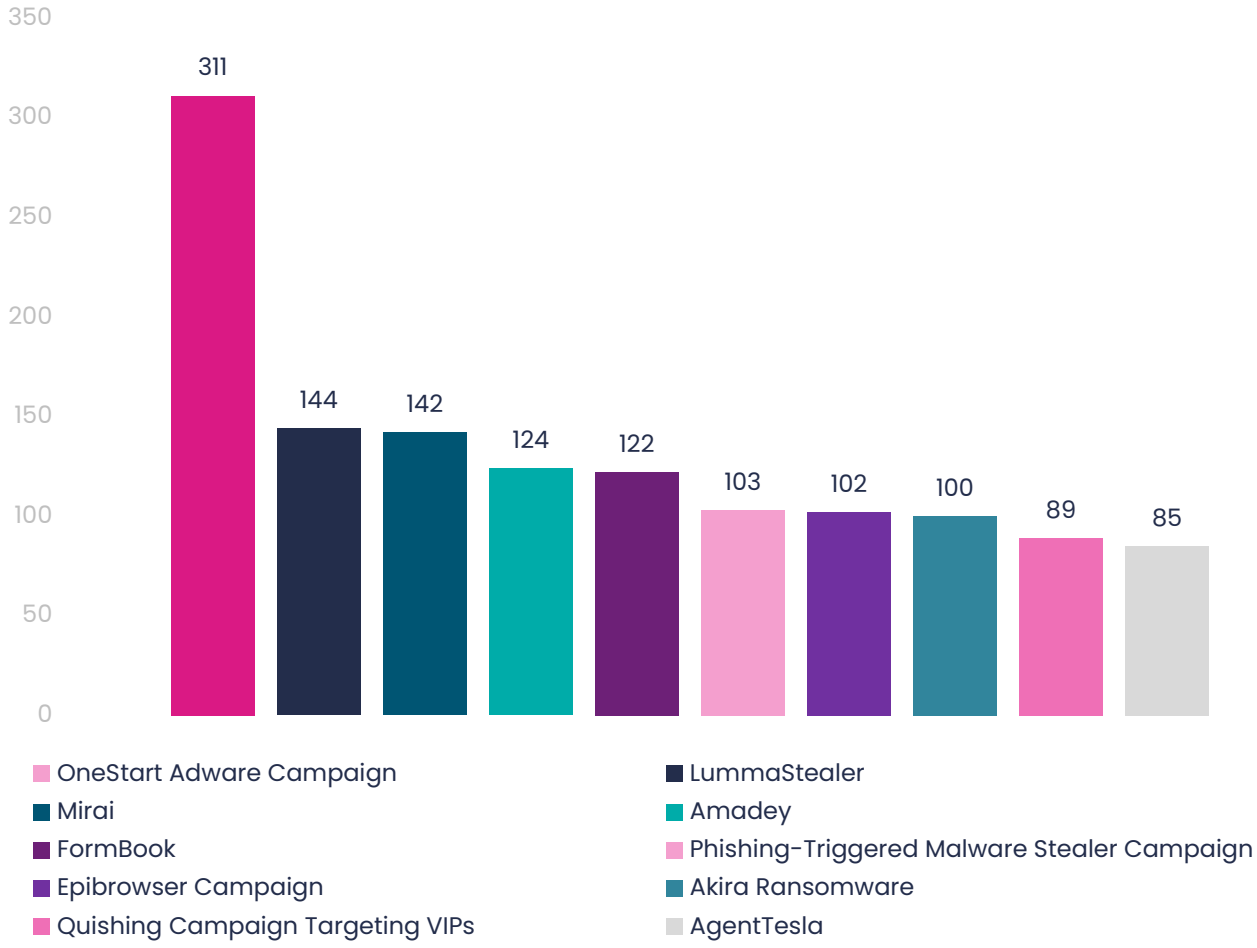
In 2025, the work of identifying Indicators of Compromise (IoC) carried out by the Threat Intelligence team increased by 34% compared to 2024. In line with the objective of directing threat detection and mitigation efforts more specifically, IoC identification has focused on those types of malware that are having or could have the greatest impact on Inetum's LiveSOC customers.

In terms of quantity, the indicators of compromise identified during the campaign carried out by OneStart in the first half of the year stand out in the analysis and sharing of Indicators of Compromise, along with others related to LummaStealer, Mirai, Amadey and Formbook identified in the second half of the year.

Number of IoC and types of malware in 2024 and 2025



Top 10 most shared IoC by type by the Threat Intelligence team in 2025



06

Strategic Alliances

Since its establishment, Inetum's LiveSOC has formed partnerships with various suppliers and public and private organisations, both nationally and internationally, with the aim of improving security posture, sharing information and identifying emerging threats in advance.

5.1 Partners and alliances

Through its LiveSOC, Inetum maintains strategic alliances with global technology leaders to strengthen its cybersecurity capabilities and offer advanced solutions to its customers. These partners include **Microsoft and Google**, which provide cloud platforms and integrated security tools; **Servicenow, Trellix, Proofpoint, Palo Alto Networks and CrowdStrike**, which provide cutting-edge technologies in endpoint protection, threat detection and response, and perimeter security; as well as **Splunk**, key to event monitoring and analysis, and **Recorded Future**, a leader in threat intelligence, among others.

5.2 National SOC Network (Spain)

The National SOC Network (RNS), of which Inetum's LiveSOC is a part, is a tool for coordinating collaboration and information exchange between Cybersecurity Operations Centres (SOCs) throughout the country, whether public or private, launched by the CCN-CERT[25].

5.3 ICARO Project (Spain)

Since 2025, Inetum's LiveSOC, thanks to its collaboration with AMETIC, has been one of the organisations participating in the ICARO Project, launched by INCIBE, for the sharing of Indicators of Compromise in a common MISP, with feedback and limited access to International CERTs, strategic operators and institutions affiliated with RedIRIS[26].

5.4 FIRST (International)

FIRST has more than 800 members across Africa, America, Asia, Europe and Oceania. The organisation works with incident response teams to improve both reaction and prevention, promoting cooperation, coordination and information sharing among its members in order to strengthen global capacity in the face of cybersecurity incidents[27].

[25] National SOC Network, RNS: https://rns.ccn-cert.cni.es/

[26] ICARO Project: https://www.incibe.es/incibe-cert/servicios-operadores/icaro

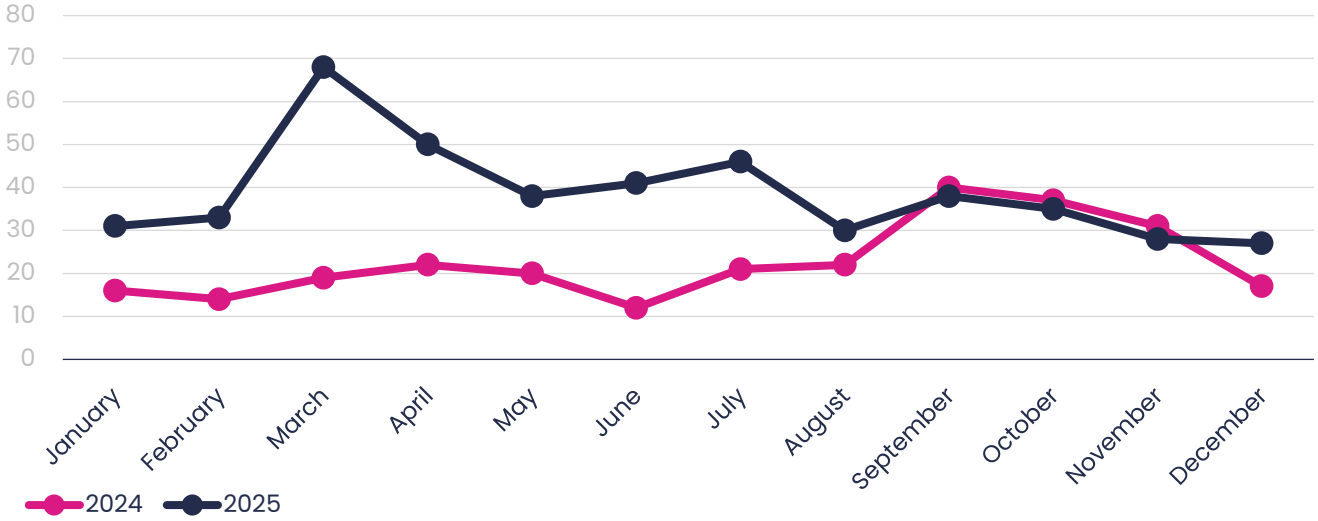
[27] FIRST: https://www.first.org/

07

Deliverable products

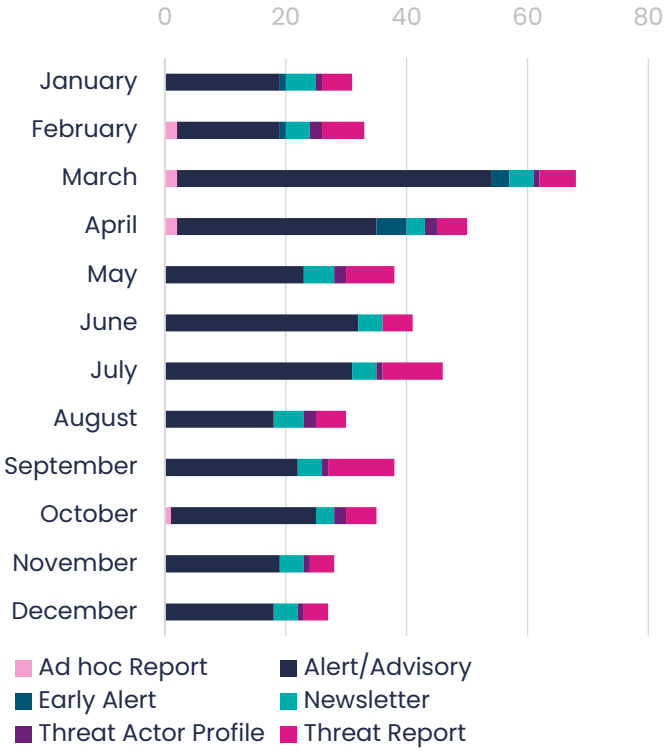
During 2025, the Threat Intelligence team's deliverable products have focused on monitoring daily alerts on vulnerabilities, emerging threats, ongoing campaigns, new attack techniques, and compilations of news items of interest, among others. The number of products delivered increased by 72% compared to 2024 (rising from 271 to 465), primarily due to an increase in the number of monitored technologies, with the most notable rise occurring between March and July.

Product delivery comparison: 2024 vs. 2025

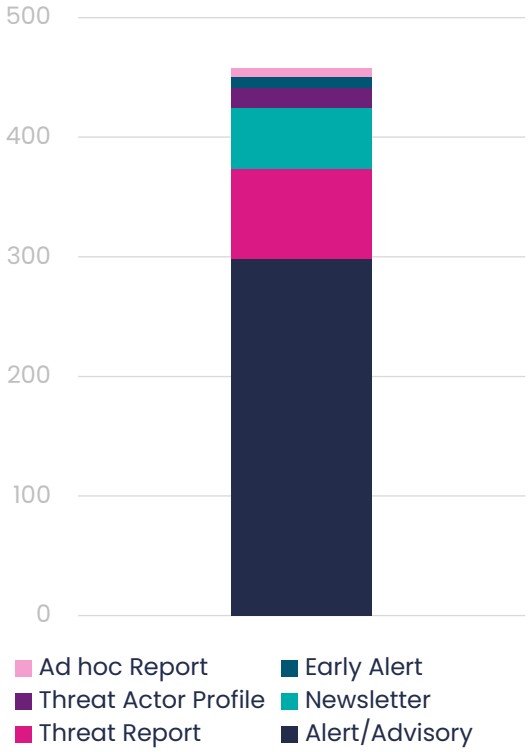


In 2025, alerts and advisories were the most frequently delivered products for the distribution of each type of product per month.

Monthly distribution by type of product delivered



Annual distribution by type of product delivered



08

2026 Trends

GLOBAL SITUATION

Geopolitical dynamics suggest that armed conflicts will continue to influence the global landscape, with hybrid warfare emerging as a means for both state and non-state actors to assert their influence. The combination of military operations, cyberattacks on critical infrastructure, disinformation and hacktivism campaigns, and cyber espionage will persist. The systematic use of cyber capabilities to influence political processes could amplify instability, with economic repercussions.

Meanwhile, friction between the United States and Europe could intensify due to the National Security Strategy questioning the political and economic resilience of the continent and its ability to sustain strategic alliances. Washington could press for Europe to take on greater responsibility for defence and technological autonomy. Against this backdrop, the EU is expected to strengthen its defensive and legislative measures, as evidenced by initiatives such as the REARM Plan. These initiatives are aimed at bolstering military and cyber capabilities, as well as strategic production, with the ultimate goal of reducing external dependence.

THREATS

- In 2026, ransomware is likely to remain one of the most profitable threats, with double or triple extortion tactics affecting public and private entities alike.
- The use of 'as-a-service' models for any type of threat will continue to increase due to the ease with which attacks can be carried out without prior knowledge or skills.
- State-sponsored APT groups could intensify operations against critical sectors in line with military conflicts.
- DDoS attacks are likely to increase in volume and sophistication, driven by IoT botnets and illicit services that facilitate the saturation of essential infrastructure.
- Digital identity could emerge as a priority target for attackers. Attacks against authentication mechanisms, including MFA bypass and identity provider exploitation, will increase, as will credential compromises.
- Phishing campaigns will become more targeted and automated using AI, combining techniques such as spear-phishing and quishing to maximise effectiveness and evade traditional controls. Advanced identity protection and proactive detection strategies will be required to mitigate these emerging risks.

TECHNOLOGICAL DEVELOPMENTS

Technological trends suggest that artificial intelligence will play a pivotal role in both defence and attack strategies. Adversaries could use AI to automate phishing campaigns, optimise evasion techniques, and create content for influence operations. At the same time, defensive teams will need to implement AI-powered analysis for autonomous responses. However, risks will not be eliminated; for example, those associated with AI-powered malware will require more advanced controls.

Meanwhile, post-quantum cryptography is set to become a strategic priority in light of advances in quantum computing. The adoption of quantum-resistant algorithms is likely to accelerate in anticipation of a critical transition that will ensure long-term confidentiality. However, this change could pose operational and regulatory challenges, necessitating migration plans and global standards to ensure interoperability.

inetum.

inetum.com