inetum.

Mid-Year Threat Landscape 2025

LiveSOC Inetum

Index

01

Belgium Context

The **cybersecurity landscape** in the first half of the year, both for **Belgium and the other EU countries, has been marked by ongoing military conflicts**. Support for Ukraine has meant being targeted by organisations such as NoName057(16). Other cyberthreats are ever-present, such as financially motivated threats like Medusa, RansomHub or LockBit derivatives, or state-sponsored ones like Lazarus (linked to North Korea).

Any statement or sanction issued by an EU member can trigger digital retaliation against servers physically located in Belgium, making the country a recurring target for pro-Russian hacktivist groups such as NoName057(16). In the second half of 2024, **NoName057(16) launched a sustained two-week DDoS campaign** that intermittently disrupted parliamentary, municipal, and media portals ahead of local elections. In October 2024, the group escalated its efforts by taking offline Febelfin, the Economy Ministry, and the Centre for Cybersecurity Belgium. Similar campaigns resurfaced during the 2024 EU elections, highlighting Belgium's vulnerability as a symbolic and strategic target within the EU.

The Centre for Cybersecurity Belgium shared a report[1] where they presented data from the last quarter of 2024 and the first of 2025, stating that **reports of cyber incidents increased by 80%, amount that is expected to grow in the coming years**. In the past events of 2024, threat actors have demonstrated the ability to paralyse rail traffic by taking down the NMBS/SNCB ticketing platform in January 2024, and to disrupt maritime flows via coordinated hits on the ports of Antwerp-Zeebrugge, Liège and other terminals in October 2024. Critical infrastructure provides large blast-radius opportunities for ransomware groups such as RansomHub, or LockBit and later derived groups, while hacktivists view them as highly visible levers for political pressure.

Brussels concentrates EU-level regulators, such as CINEA, REA, EISMEA, EACEA, ERCEA, HADEA[2] or the European Commission and European Council[3], and several commercial and clearing houses making Belgian networks an appealing entry point into the European payments' backbone. **ENISA** (European Union Agency for Cybersecurity) **counted nearly 500 publicly reported incidents** in the continental finance sector between 2023 and mid-2024, with **Belgium repeatedly named among the affected states**[4].

Belgium's dense concentration of biotech labs, EU health agencies and technology suppliers exposes healthcare and software supply-chain assets to both profit-drive and state-sponsored actors. Medusa's 2024 breach of Brussel's based IT firm Prosolit[5] illustrated how compromising a service provider can cascade into public hospitals, while Check Point observed **Belgian healthcare organisations absorbing an average of 2777 attacks per week** in the first quarter of 2025[6] .

Meanwhile, Lazarus continues to raid European cryptocurrency platforms[7] , and seeks biomedical research and development, making Belgian pharma and fintech startups particularly attractive. In the first half of 2025 there are records of groups **8base, Ransomhouse, Data Carry Ransomware, Sarcoma Ransomware, and Akira**, while the affected industries have been IT, travel, government, manufacturing, and industrial equipment.

1.1 International Context

Inetum is a multinational organisation offering mainly **digital services**. It has a strong presence

[1] CCB news https://ccb.belgium.be/recent-news-tips-and-warning/largest-cyber-security-operation-ever-belgium-2410-organizations
[2] EU agencies https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:eu_agencies
[3] EU institutions https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/types-institutions-and-bodies_en
[4] https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf
[5] https://www.ccinfo.nl/menu-nieuws-trends/cyberaanvallen-weekoverzichten/2032828_slachtofferanalyse-en-trends-van-week-36-2024
[6] https://itdaily.com/news/security/cyberaanvallen-belgium-software-most-targeted
[7] https://securityaffairs.com/174514/cyber-crime/lazarus-stole-1-5b-from-bybit-cryptocurrency-heist.html

in **19 countries**: Belgium, Brazil, Bulgaria, Colombia, France, India, Ireland, Luxembourg, Mexico, Morocco, Peru, Poland, Portugal, Romania, Spain, Switzerland, Tunisia, United Kingdom and United States.

In its commitment to cybersecurity and, more specifically, to **defensive security**, it has the **LiveSOC** team, which carries out its daily work for customers and at the corporate level in order to detect risks and threats early. During **the first half of 2025**, the LiveSOC team handled a total of **77,093 alerts and 25,171 incidents**.

The current global context is shaped by instability, largely due to active territorial conflicts and changes in certain political positions of the countries involved in these conflicts. **These territorial conflicts have a direct impact on the cybersecurity context and the countries involved face cyber-attacks by hacktivists and state actors**.

Throughout 2024 and early 2025 the conflict between **Russia and Ukraine** has continued with intense offensives and counter-offensives, unsuccessful in the various truce attempts promoted by the United States and leading the European Union to promote a rearmament plan. Threat actors in both countries, including hacktivists and state actors, have carried out ransomware attacks against critical infrastructure, as well as disinformation attacks aimed at destabilising systems and gathering intelligence.

The **Middle East conflict** intensified in 2024 with Israeli military operations in Gaza and the West Bank, which led to massive displacement and a humanitarian crisis during 2025, as well **as Israel, Iran and US attacks**. In the cyber realm, Israel has used cyber attacks to disable Hamas communication and defence systems, while Palestinian and Iranian groups have launched denial of service (DDoS) and phishing attacks against Israeli targets[8].

In March, threat actor 'rose87168' posted on a Dark Web forum about the **sale of 6 million Oracle records**[9]. Although Oracle did not officially confirm the security breach, some of its customers received a compromise notification from Oracle. The extent of the breach is currently unknown as no information about the source of the breach is available.

In April 2025, tensions between **India and Pakistan** escalated following a terrorist attack in Pahalgam (Kashmir), attributed by India to the Pakistani group Lashkar-e-Taiba. This episode is part of a historic conflict between the two countries since their separation in 1947, marked by territorial disputes, terrorism, nuclear rivalry and geopolitical factors. Although a cessation of hostilities was agreed on 10 May, the risk of cyber-attacks by malicious actors and APTs, as well as other possible physical retaliation, persists[10].

On 28 April 2025, a **major power outage affected Portugal and Spain, causing a significant drop in internet traffic and connectivity**. The outage also affected the quality of connectivity nationwide in Spain and Portugal[11]. On 29 April 2025, Spain's **Fábrica Nacional de Moneda y Timbre (FNMT) experienced significant problems with its digital certificate services** due to the outage. This incident affected the validation of electronic certificates, impacting the digital services of several public administrations.

Overall, **ransomware attacks have increased in the first half of the year** compared to 2024 for the 19 countries in which Inetum is present, with the United States, the United Kingdom and France being the most targeted, unchanged from last year. Also **noteworthy is the activity of advanced persistent threat** (APT)[12] actors promoted by

---

[8] *[Threat Report] Cybersecurity Context - Iran & Israel rising conflict*
[9] *[Threat Intelligence] Alert - Oracle Leak Update*
[10] *[Threat Report] Cybersecurity Implications of India Pakistan Geopolitical Tensions*
[11] *Source: https://blog.cloudflare.com/how-power-outage-in-portugal-spain-impacted-internet/*
[12] *Advanced Persistent Threats (APTs) are undetected cyber-attacks designed to steal sensitive data, conduct cyber-espionage or sabotage crucial systems over a long period of time.*

states in the current context of geopolitical instability and active armed conflicts.

Denial-of-service attacks continue to rise in the first half of 2025. Cloudflare recently reported that it mitigated 20.5 million DDoS attacks in the first quarter, a figure that nearly equals the total number of attacks blocked throughout 2024. Key **threat actors include hacktivist/state-sponsored groups** such as NoName057 with many targets in EMEA[13] in the first few months of 2025. Many of these are in the context of conflicts such as Russia-Ukraine and Israel-Iran.

Exploitation of vulnerabilities has been one of the main attack vectors for threat actors in 2024. **The trend could continue in 2025**, as the number of vulnerabilities published in the first half of the year is like that of the same period last year, with the number of exploited vulnerabilities also showing similar figures.

During the first half of 2025, marked by disruptions in critical infrastructure and a continued rise in global cyber threats, **operational resilience** became a key factor in ensuring service continuity. In this context, Inetum's LiveSOC maintained service continuity thanks to the **robustness of its mechanisms and guarantees**.

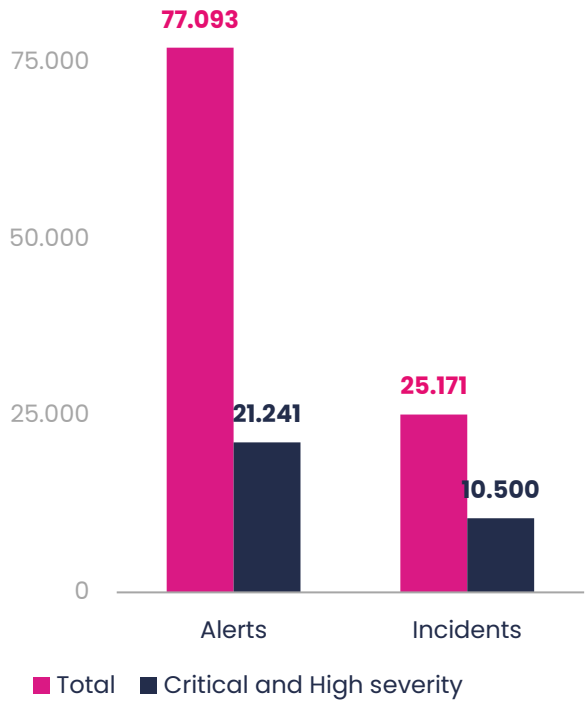
[13] *Europe, Middle East and Africa.*

02

Alerts and incidents managed

During the first half of 2025, Inetum's LiveSOC team managed a total of 77,093 security alerts[14], of which 21,241 were classified as critical or high severity. In addition, the team analyzed 25,171 security incidents[15], including 10,500 of critical or high severity, with the aim of providing insights into their occurrence and mitigation.

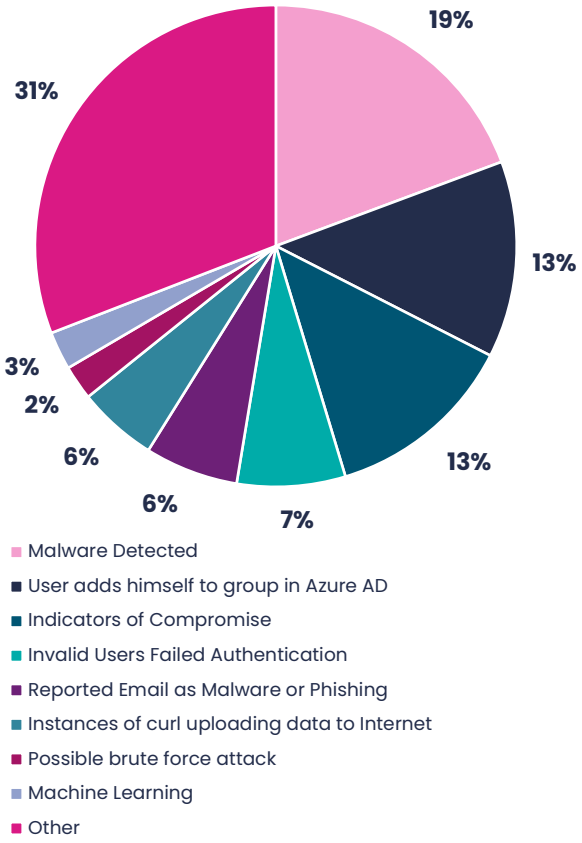
Figure 1.
Number of alerts managed by Inetum LiveSOC in the first half of 2025



Source: Own elaboration with internal data

Currently, with the figures on alerts and incidents for the first half of the year it is not possible to anticipate a clear trend for the end of 2025, also because these figures will vary by the number of clients that LiveSOC manages (potential new clients), as well as by the implementation of new detection measures that are applied within the systems (e.g. ingestion of Indicators of Compromise).

Figure 2.
Number of alerts by type managed by the Inetum SOC during the first half of 2025



Source: Own elaboration with internal data

Top 5 Alerts identified by the SOC in the first semester

1. Malware Detected

Indicates that malicious software has been identified on the system. This encompasses a range of harmful programs such as viruses, worms, trojans, ransomware, and spyware, all designed to compromise, damage, or disable computers and networks.

2. User adds himself to group in Azure AD

When a user adds themselves to a group, this action might indicate a potential privilege escalation, where the user is trying to gain more

[14] Alert: An automatic notification generated by a security system (such as a SIEM, IDS, antivirus, etc.) that indicates potentially suspicious or malicious activity.

[15] Incident: An alert that has been analysed and confirmed as a real threat or security breach.

access than they are allowed. It could also suggest that the account has been compromised, with an attacker attempting to move laterally or maintain access. Alternatively, it may point to a permissions misconfiguration that lets users change their own group memberships without proper oversight or control.

3. Indicators of Compromise

This alert is triggered when the SOC's detection tools, fed by data collected by the SOC teams, identify digital evidence suggesting a potential security breach. IOCs include unusual traffic patterns, unauthorized changes, and suspicious files, among others.

4. Invalid Users Failed Authentication

Triggered by failed authentication attempts from invalid users. This indicates that unauthorized users or users with incorrect credentials are trying to access the system, which can be a sign of attempted unauthorized access or brute force attacks.

5. Reported Email as Malware or Phishing

Generated when it reports an email as malware or phishing. Phishing emails attempt to trick users into revealing personal information or installing malware.

Special mention should be made of the **alerts detected on Epibrowser and Onestart, with a large increase during the month of March**, on which the Threat Intelligence team carried out the respective analyses and shared them in Malware Report format[16]. The detection of these alerts in the systems was carried out thanks to the indicators of compromise identified and disseminated by said team.

[16] *[Threat Intelligence] Malware Report – Onestart and [Threat Intelligence] Malware Report - Epibrowser*

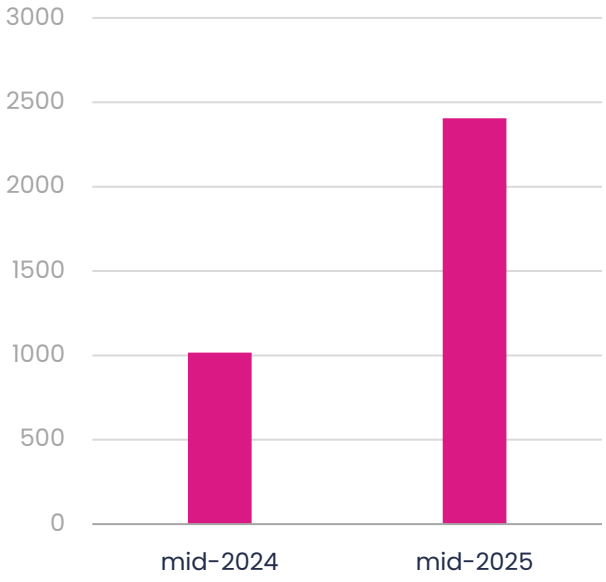
03

Main Threats

3.1 Ransomware

Ransomware attacks have increased in recent years, as reflected in the Threat Landscape 2024, which mentioned that ENISA (European Union Agency for Cybersecurity) highlighted this threat as one of the main threats at European level. Globally, it is also one of the most prominent threats, with an **appreciable upward trend in the first half of 2025**, in the 19 countries where Inetum is present, with a total of 2,406 attacks.

Figure 3.
Number of ransomware attacks in the first half of 2024 and 2025, for the 19 countries where Inetum is present



Source: Own elaboration based on Recorded Future data.

Taking into account the 19 countries in which Inetum is based, a comparison of the top 10 countries victim of this type of threat during the first six months of 2024 and 2025 is made, showing that the top 4 remains unchanged, and identifying some small changes in the following positions.

Top 10 Victim Countries 2025


= **United States**


= **United Kingdom**


= **France**


= **Spain**


+1 **Brazil**


-1 **India**


+1 **Mexico**


+1 **Belgium**

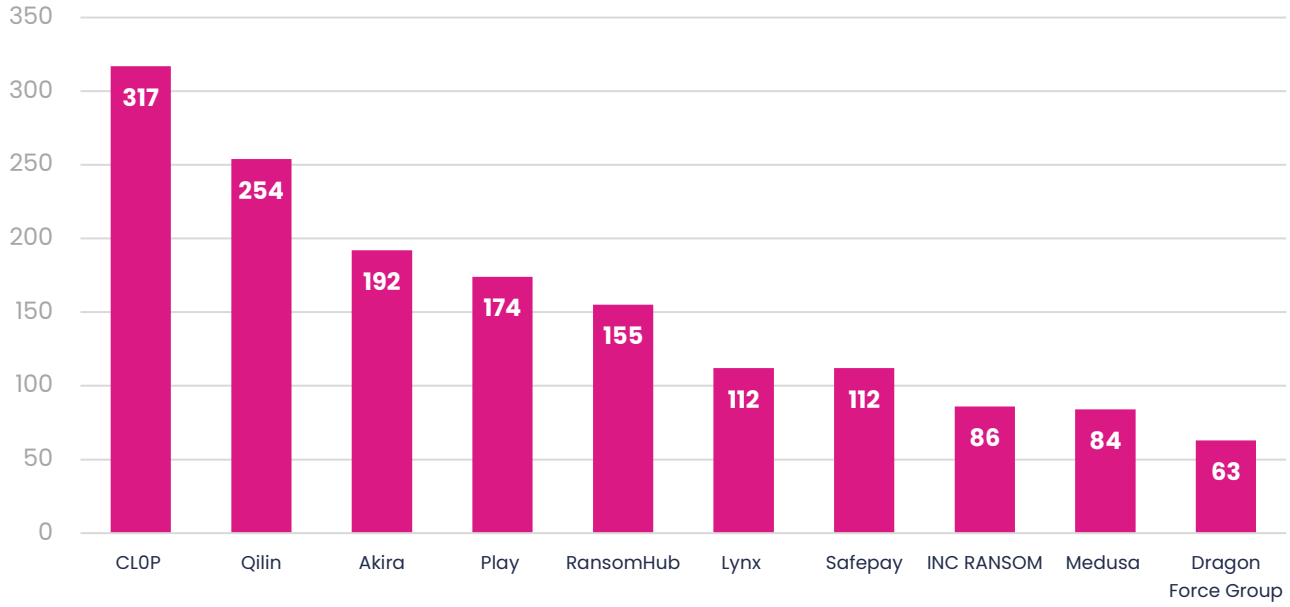

-2 **Switzerland**


+4 **Colombia**

The most active ransomware actors in the first half of 2025 included Cl0p, Qilin, Akira, Play and RansomHub. In total, attacks from 99 different ransomware actors have been identified, indicating the wide variety of threats facing the organisations managed by the LiveSOC team.

Figure 4.

TOP 10 ransomware groups by number of attacks in the first half of 2025, for the 19 countries in which Inetum has a presence



Source: Own elaboration based on Recorded Future data.

During the first half of 2025, the Threat Intelligence team published six profiles of ransomware actors[17], selected based on their impact on the cybersecurity landscape. The prioritisation was based on criteria such as the volume of malicious activity observed, the adoption of novel techniques or the targeting of strategically relevant sectors.

3.2 Advanced persistent threats

An Advanced Persistent Threat (APT) is a sophisticated and prolonged type of cyberattack whose main objective is to infiltrate a specific network in order to **steal sensitive information, conduct espionage or sabotage critical systems**, all without being detected[18].

[17] *[Threat Actor Profile] – Cl0p Ransomware, [Threat Actor Profile] – FOG Ransomware, [Threat Actor Profile] – Lynx Ransomware, [Threat Actor Profile] – Medusa Ransomware, [Threat Actor Profile] – Qilin Ransomware and [Threat Actor Profile] – SafePay Ransomware*

[18] *Source: https://www.ibm.com/es-es/topics/advanced-persistent-threats*

APTs, in the current geopolitical context with several active armed conflicts, are of great importance as many of them are related to states, such as China or Russia.

In this regard, Inetum's Threat Intelligence team has published two profiles of APT[19] actors in the first half of the year, which are of interest due to the sectors they attack and their high level of activity:

APT29

APT29, also known as Cozy Bear or The Dukes, is a **cyber-espionage actor linked to Russian intelligence**. With registered activity since at least 2014, this group has carried out intrusions in key sectors such as **government institutions, healthcare, education, the financial sector, telecommunications, the energy industry and defence**. Its presence has been detected in different regions of the world, including North America, Europe, Asia, Africa and South America, demonstrating its global operational capabilities.

APT41

APT41, also known as Double Dragon, is a sophisticated and prolific threat actor dedicated to both **espionage and financially motivated cybercrime with ties to China**. 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 in various sectors.

3.3 Denial of service

A Distributed Denial of Service (DDoS) attack aims to disrupt the normal operation of an online service, such as a website, application or digital platform. It is done by saturating system resources, such as bandwidth or server capacity, by sending a huge amount of traffic from multiple sources at the same time.

In the first quarter of 2025, Cloudflare blocked a total of 20.5 million DDoS attacks, while 21.3 million DDoS attacks were blocked in the whole of 2024[20]. These figures demonstrate **the rise of these attacks and the increased activity of malicious actors such as NoName057**. Based on this trend, the Threat Intelligence team published six Threat Reports in the first half of the year[21].

3.4 Vulnerabilities

Vulnerabilities are an important part of risk management and their exploitation is one of the main attack vectors. For vulnerability management, the **CVE** (Common Vulnerabilities and Exposures), a unique identifier assigned to a known security vulnerability, is used as part of the standardised system.

To count the number of published vulnerabilities of CVEs, one of the most used is the US database **NVD** (National Vulnerability Database) of the **NIST** (National Institute of Standards and Technology) [22]. This database not only contains all published CVEs, but also information on severity, affected products and links of interest.

Looking at the NIST records, during **the first half of 2025 there are no notable variations in the number of published vulnerabilities compared to 2024,** with the number of CVEs in 2024 and 2025 in the first six months being similar.

---

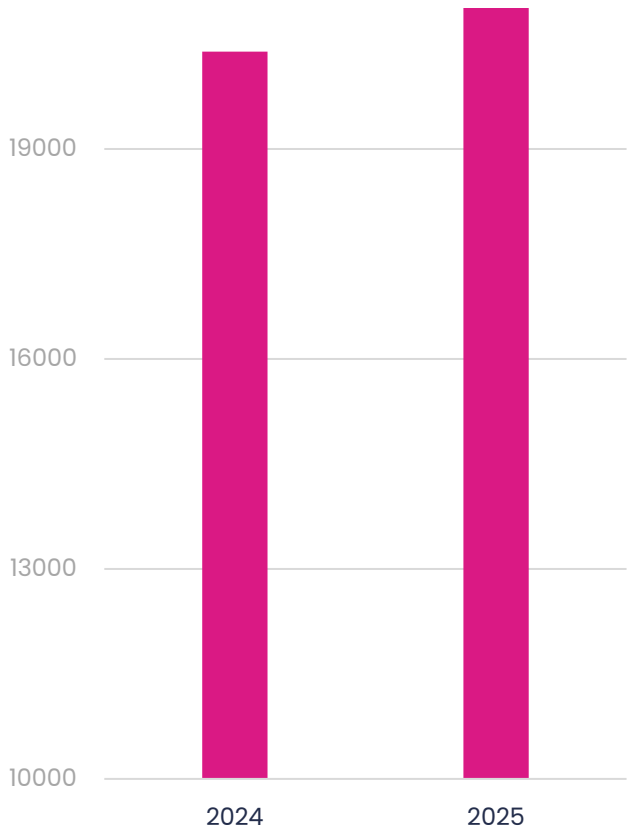
[19] *[Threat Actor Profile] – APT29 and [Threat Actor Profile] – APT41*

[20] *Source: https://radar.cloudflare.com/reports/ddos-2025-q1*

[21] *[Threat Report] DDoS Campaign Proliferation, Vectors and Actors Involved, [Threat Report] NoName057, [Threat Report] NoName057 targeting french entities, [Threat Report] NoName057 targets German and new French entities, [Threat Report] Nuevos ataques de NoName057 and [Threat Report] DDoS Campaign against Spain entities*

[22] *US government agency that is part of the Department of Commerce. Its primary mission is to promote innovation and industrial competitiveness by advancing measurement science, standards and technology.*

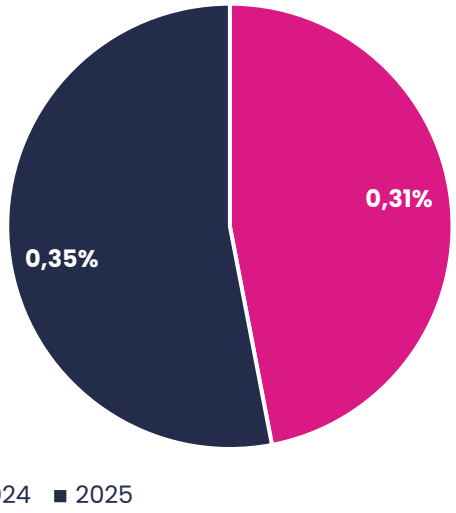
Figure 5.
Number of vulnerabilities at NIST in the first half of 2024 vs. 2025



Source: https://nvd.nist.gov/vuln/search?results_type=statistics&search_type=all&form_type=Basic&isCpeNameSearch=false

The trend in the identification of **exploited vulnerabilities would also remain stable**, with the first half of 2025 showing similar figures to the same period in 2024 according to information gathered by NIST based on publications by CISA (Cybersecurity and Infrastructure Security Agency: America's Cyber Defense Agency). In the first six months of 2024, a total of 64 vulnerabilities were identified as exploited (0.31% of the vulnerabilities published in that period), in 2025, a total of 83 vulnerabilities (0.35% of the vulnerabilities published in that period).

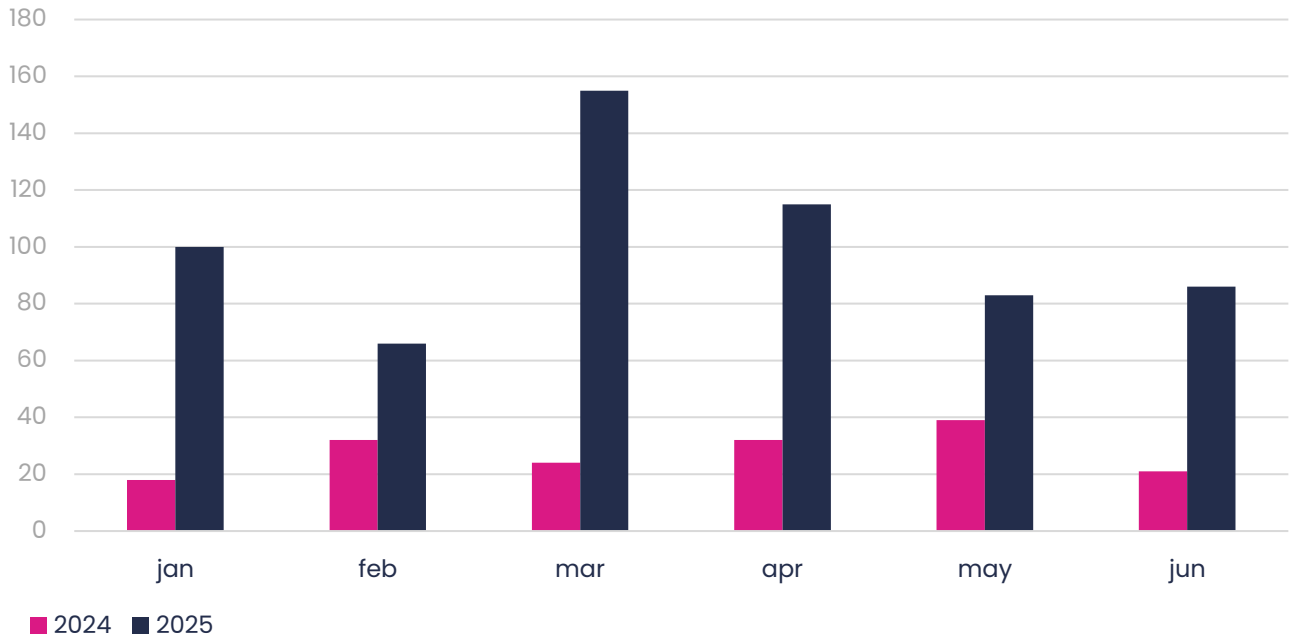
Figure 6.
Percentage of exploited vulnerabilities out of total vulnerabilities published in the first half of 2024 vs. 2025



Source: https://nvd.nist.gov/vuln/search/statistics

Despite the similarity of the figures in terms of the publication of vulnerabilities and exploited vulnerabilities, the Threat Intelligence team, during the first half of the year 2025, and related to the increase of technologies to monitor for our clients, **has considerably increased the number of CVEs shared** with them, in the form of Alerts, Advisories or Reports.

Figure 7.
Comparison by month 2024 vs. 2025 of shared CVEs



Source: Own elaboration with internal data.

04

Tactics and Techniques

The **MITRE ATT&CK** (Adversarial Tactics, Techniques, and Common Knowledge) framework is a globally accessible knowledge base that documents in a structured way the behaviour of real cyber adversaries around the tactics and techniques they use[23].

In this context, during the first half of 2025, out of the total number of alerts and incidents managed and analysed by Inetum's LiveSOC, four types of alerts and incidents have been selected as relevant to be linked to specific techniques of the framework, as well as some of the actors using them.

This correlation between alerts, incidents and techniques and tactics allows not only to better understand the attacker's behaviour, but also to prioritise responses and strengthen defensive controls based on real and documented threats.

Alert	Technique	Tactic	Description	Actor
Reported Email as Malware or Phishing	**T1566.001 Phishing: Spearphishing Attachment**[24]	TA0001: Initial Access	Emails with malicious attachments designed to trick the user into executing code or stealing credentials.	AgentTesla, Lumma Stealer, Gamaredon, Kimsuky, multiple APTs
Malware Detected	**T1204.002 User Execution: Malicious File**[25]	TA0002: Execution	The adversary relies on the user opening a malicious file to execute code. This can be a .doc, .pdf, .exe, etc.	Multiple APTs, Black Basta, Andariel, Agent Tesla, GuLoader, FIN7
Invalid Users Failed Authentication	**T1110.001 Brute Force: Password Guessing**[26]	TA0006: Credential Access	Failed attempts at authentication of invalid users, which may indicate brute force attacks or unauthorised access.	Emotet, APT28, APT29, FIN6
Instances of curl uploading data to Internet	**T1048.003 Exfiltration Over Alternative Protocol: Unencrypted /Obfuscated Non-C2 Protocol**[27]	TA0010: Exfiltration	Use of tools such as curl to upload data outside the corporate environment without encryption or using non-standard protocols.	Agent Tesla, Salt Typhoon, Lazarus, APT32, APT33

[23] *Source: https://attack.mitre.org/*
[24] *Source: https://attack.mitre.org/techniques/T1566/001/*
[25] *Source: https://attack.mitre.org/techniques/T1204/002/*
[26] *Source: https://attack.mitre.org/techniques/T1110/001/*
[27] *Source: https://attack.mitre.org/techniques/T1048/003/*

Incident	Technique	Tactic	Description	Actor
User access multiple workstation	**T1078.004 Valid Accounts: Cloud Accounts**[28]	TA0001: Initial Access	Using valid accounts in cloud environments to gain initial access.	APT29, APT5, LAPSU$S
WmiPrvSe.exe Rare Child Command Line	**T1047 Windows Management Instrumentation**[29]	TA0002: Execution	Using WMI to remotely execute commands or scripts.	APT29, Akira, Lazarus, Volt Typhoon, Sandworm, INC Ransomware
Audit log cleared	**T1070.001 Clear Windows Event Logs**[30]	TA0005: Defense Evasion	Clearing Windows event logs to hide traces of malicious activity.	APT41, LockBit, RansomHub, Play
Failed Authentication via Kerberos	**T1110.003 Brute Force: Kerberos**[31]	TA0006: Credential Access	Repeated authentication attempts against Kerberos services to guess valid passwords.	APT28, APT29, FIN6, Lazarus Group, Cobalt Group

[28] *Source: https://attack.mitre.org/techniques/T1078/004/*
[29] *Source: https://attack.mitre.org/techniques/T1047/*
[30] *Source: https://attack.mitre.org/techniques/T1070/001/*
[31] *Source: https://attack.mitre.org/techniques/T1110/003/*

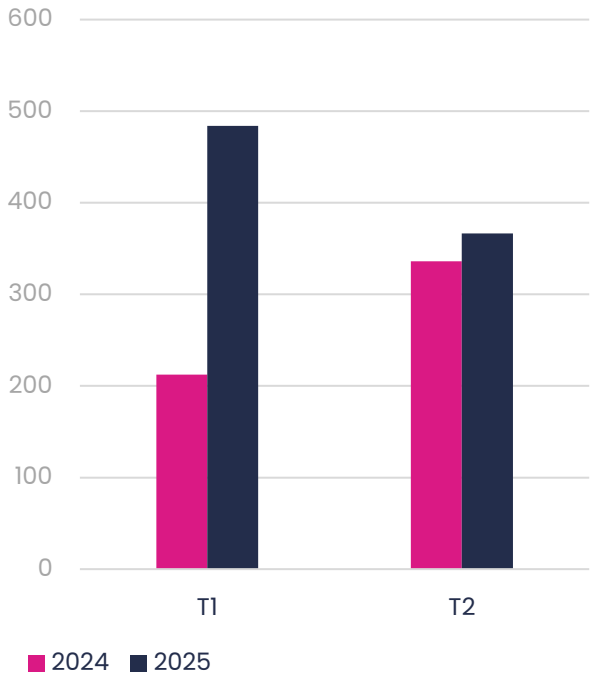
05

Indicators of Compromise

Indicators of Compromise serve to identify attempts to compromise own systems and customers. The work of identification, analysis and inclusion in detection systems prevents such attempts to compromise organisations. From the Threat Intelligence team, these indicators of compromise are transferred to other teams, as well as to the SOC National Network (RNS)of Spain, of which Inetum is part of as a Gold level partner.

LiveSOC, as a **Gold level collaborator of the RNS**, has contributed to the sharing of indicators of commitment during the first half of the year as usual, in this case, an increase in the score received from these indicators is seen, related to the type of indicators shared based on the RNS system, since depending on the type of indicator of compromise this has one score or another.

Figure 8.
RNS score for Inetum SOC for the first two quarters of the year, 2024 vs. 2025

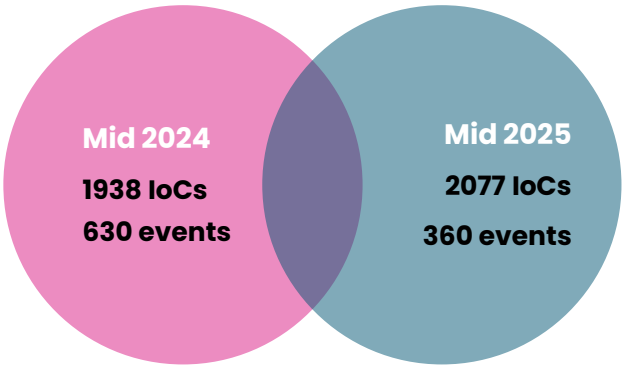


Source: Own elaboration with data from the RNS

As observed in the section on Alerts and Managed Incidents, a large number of alerts are related to the identification of indicators of compromise in the detection tools used by Inetum's SOC. This is an example of the importance of identifying, analysing and including them, as their early detection prevents them from becoming security incidents.

In the first half of 2025, compared to 2024, a figure very close to that of 2024 has been identified, analysed and shared. In terms of events created, there is a variation in 2024, determined by the large number of campaigns registered in the first half of this year from which a large number of indicators of Compromise could be identified, such as those of Onestart and Epibrowser.

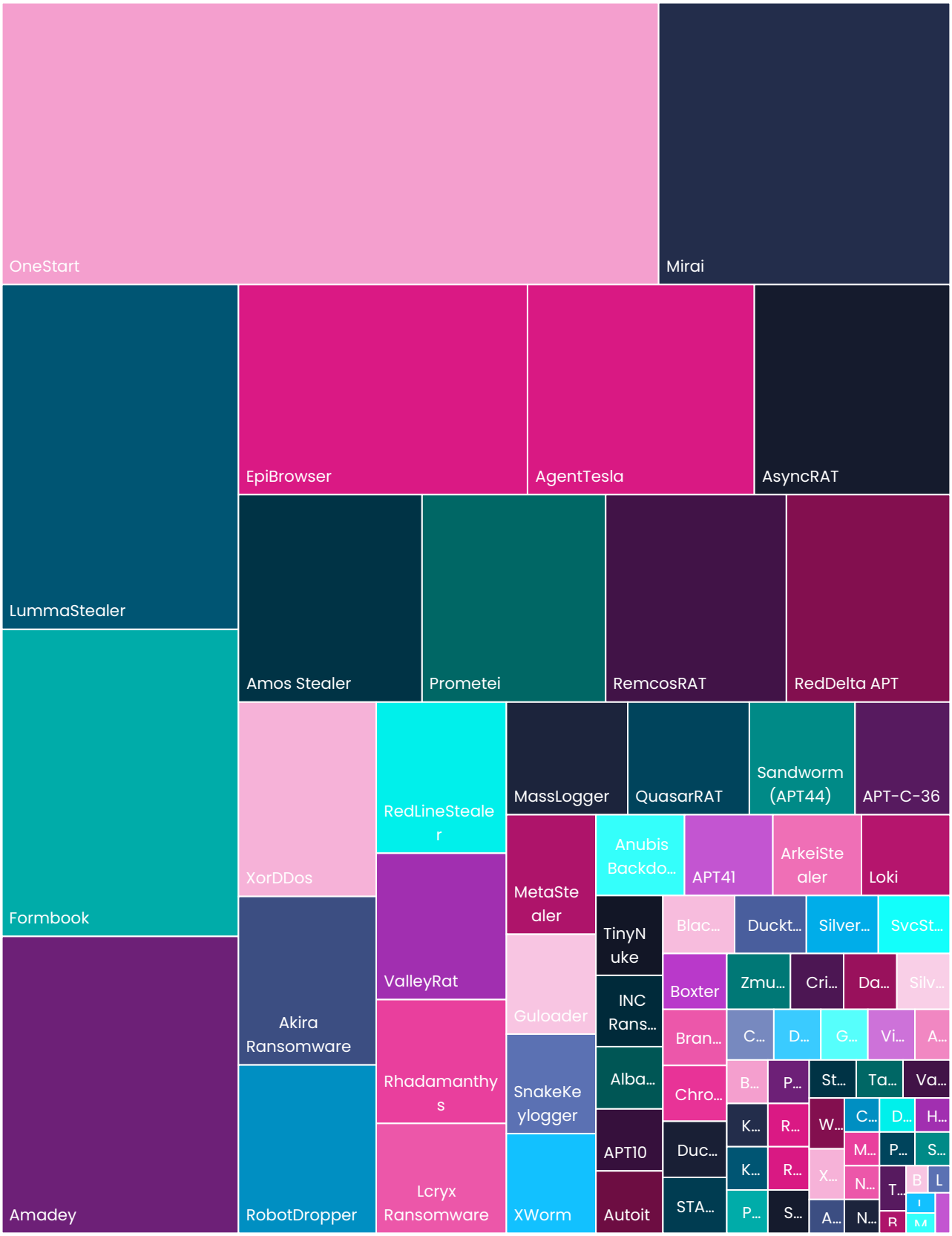
Figure 9.
Number of Indicators of Compromise/Shared Events first semester 2024 vs. 2025



Source: Own elaboration with internal data.

Of the indicators identified and shared by the Threat Intelligence team**, adware, botnets, stealers, Trojans, RATS and to a lesser extent ransomware and APTs**. The identification of indicators of compromise is complex and requires validation and consultation of a large number of sources, as well as their relationship with other indicators of compromise for the detection of specific campaigns, all with the requirement of timeliness, in order to improve early detection. In addition, the difficulty of identifying indicators of ransomware and APTs is noteworthy, given that publicity of these incidents is often scarce, including the victim's knowledge of the attack itself.

Figure 10
Type of malware by number of Indicators of Compromise identified



Source: Own elaboration with internal data.

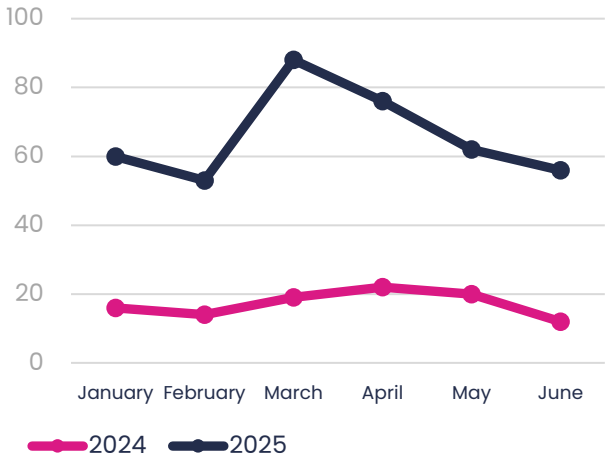
06

Deliverable products

Given the particularity of the current scenario, in which the exploitation of vulnerabilities for access to systems is one of the most common attack vectors for organizations, at the beginning of 2025 the Threat Intelligence team considered the need to expand the number of monitored technologies, with an increase of 141% compared to 2024, with the aim of identifying the maximum number of published vulnerabilities and transferring this valuable information to clients.

The increase in technologies monitored in the first half of the year has influenced the number of products delivered, in Alert, Advisory and Report formats, by the Threat Intelligence team. This increase is considerable when compared to the products delivered during the first six months of 2024.

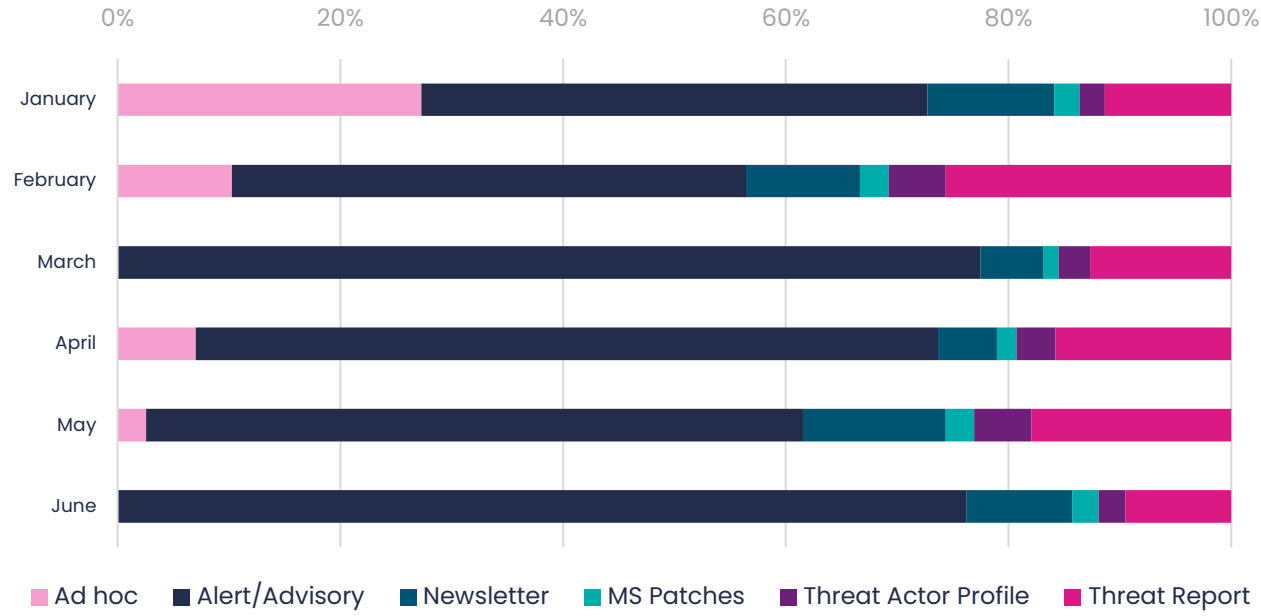
Figure 11. Comparison of products delivered 2024 vs. 2025



Source: Own elaboration with internal data.

At the same time, the other formats of products delivered have also increased, identifying a greater number of topical issues of interest to CSS customers. The distribution of the type of products delivered in each month of the first half of 2025 was as follows:

Figure 12.
Number of product type delivered per month in 2025



Source: Own elaboration with internal data

07

Trends Assessment 2025

In the Threat Landscape 2024 document, released at the beginning of 2025, a series of topics of interest to the field of cybersecurity were analysed and presented, based both on information acquired by the LiveSOC department in its daily development, as well as on external and reputable sources of information. Thus, after analysing the topics, an approximation of their trends for 2025 was made.

In this first half of 2025, and by reviewing the identified thematic areas for the same period in 2024, it has been possible to assess whether this anticipation of trends in the Threat Landscape 2024 had been fulfilled to a greater or lesser extent. Below is a table assessing the accuracy of the predictions made by the Threat Intelligence team for 2025. Overall, these predictions have proven to be accurate in the context of the first half of the year.

Comparison

As predicted in the 2024 Threat Landscape on trends for 2025, the international cybersecurity landscape has continued to experience an increase in the number of attacks, particularly denial-of-service (DoS) and ransomware attacks.

Denial-of-service attacks not only continued, but increased very considerably compared to 2024, influenced and contingent, as identified in the Threat Landscape, on the progress of conflicts, as they increase or decrease in severity and impact of the Russia/Ukraine and Iran/Israel conflicts.

Ransomware has maintained its upward trend as anticipated, with the emergence of new groups with a high attack and affectation capacity; Ransomware as a Service (Raas), which is becoming increasingly common in the current scenario, stands out.

RAT malware, stealers and adware, among others, have maintained their 2024 trend, continuing to affect systems and being used as a tool in attacks carried out by a large number of malicious actors such as APTs, with repercussions due to their links with states and in the context of various international conflicts.

Both the identification of vulnerabilities and their exploitation, zero-days, have remained stable in the first half of 2025 compared to the same period in 2024, this trend could continue or increase, due to their frequent use as an initial access vector by malicious actors.

Regarding the use of Artificial Intelligence, its offensive use for automating attacks, creating malware and misinformation has continued, making it difficult for cybersecurity teams to anticipate and mitigate. Despite this, its defensive use has also increased, with various security vendors and large technology companies using it to improve early detection, with automated responses and the use of predictive analytics.

Area	2025 Prediction	Evaluation
General Context	✔	☑ Very accurate
DDOS	✔	☑ Very correct
Ransomware	✔	☑ Excellent
RATs and Stealers	✔	☑ Very good
Zero-day vulnerabilities	✔	☑ Accurate
Artificial Intelligence	✔ Partial	☑ Acceptable

inetum.

inetum.com