inetum.

Threat Landscape 2024

LiveSOC Inetum

Index

01

Global Context

The international landscape is characterized by **increasing tension between rival powers and the intensification of regional conflicts**. Social polarization and distrust between nations have exacerbated existing rivalries, redefining global power dynamics. In this context, the competition for economic, technological, and strategic influence has become the central axis of international relations.

In 2024, **cyberspace has solidified as a battleground for geopolitical tensions**, particularly in the conflicts between Russia-Ukraine, China-Taiwan, and Israel-Iran. In this regard, cybersecurity is not exclusively a defensive barrier, but a weapon used to destabilize economies, manipulate information, and project political power.

DoS attacks are a common tactic to saturate and paralyze critical infrastructures. Russian state actors employ these techniques to destabilize the Ukrainian economy and undermine confidence in its institutions. These attacks are often accompanied by cyber espionage campaigns aimed at gaining prolonged access and extracting valuable information by APTs.

The theft of strategic data is used to weaken the rival and bolster internal capabilities. Stealers[1] play a fundamental role by enabling prolonged intrusions and access to critical networks. In this sense, espionage operations, especially from China, are directed at stealing intellectual property and key data in strategic sectors of their competitors, such as Taiwan, weakening its technological position and preparing the ground for possible reunification. **The most targeted sectors this year include technology, professional and consulting services, and healthcare**, reflecting the pursuit of a competitive and geopolitical advantage in sensitive areas.

On the other hand, **Artificial Intelligence (AI) emerges as a significant threat** in this dynamic, increasing offensive capabilities in cyberspace. Advanced algorithms identify vulnerabilities in real-time while automating cyber espionage attacks on an unprecedented scale and perfecting disinformation campaigns with precision. Additionally, their ability to produce high-quality fake content and manipulate narratives on a large scale complicates threat detection, allowing covert operations with a destabilizing impact. The United States and China lead this field, competing to develop systems that redefine the balance of power and increase global risks of digital instability and prolonged conflicts.

[1] *A stealer is a trojan that collects information from a system. The most common form is to gather login information, such as usernames and passwords, and then send the information to another system. Other stealers, called keyloggers, record the user's keystrokes, which can reveal confidential information.*

Concurrently, the use of ransomware remains a selective high-impact threat. Unlike previous massive campaigns, attacks are directed at high-value targets to generate economic pressure and compromise key sectors. This strategy generates revenue that funds cover operations and serves as a mechanism for political destabilization, forcing affected states to negotiate or redirect resources. This situation applies to pro-Iranian hacktivist groups and Israeli attacks on Tehran's nuclear infrastructure.

Control over strategic sectors is fundamental, as it represents a critical economic and geopolitical advantage. Simultaneously, disinformation campaigns aim to fragment societies, delegitimize governments, and politically pressure rivals. This combination of offensive and defensive tactics underscores the multidimensional nature of cyber warfare, focused on control and deterrence.

Cyberspace redefines global competition. The ability to infiltrate, manipulate, or destroy key digital systems becomes a true indicator of power. In this context, states that control this domain could dictate the rules of the game, using access to data, information manipulation, and digital sabotage as essential parts of their strategy.

02

Region and Sector

Inetum's SOC Department works with clients located in Europe and mainly in Spain. These clients are both public and private organizations and belong mainly to the following sectors:

GOVERNMENTAL	INDUSTRIAL - MANUFACTURING	FOOD
LOGISTICS	ENERGY	TECHNOLOGICAL

Among the most prominent security incidents this year, for the sectors to which Inetum's SOCcustomers belong, and the regions in which they are located, the following threat actors stand out:

LOCKBIT, CL0P, ALPHV/BLACKCAT, HIVE, CONTI

LOCKBIT & RANSOMHUB

LOCKBIT & RANSOMHUB

ALPHV/BLACKCAT

CACTUS & LOCKBIT

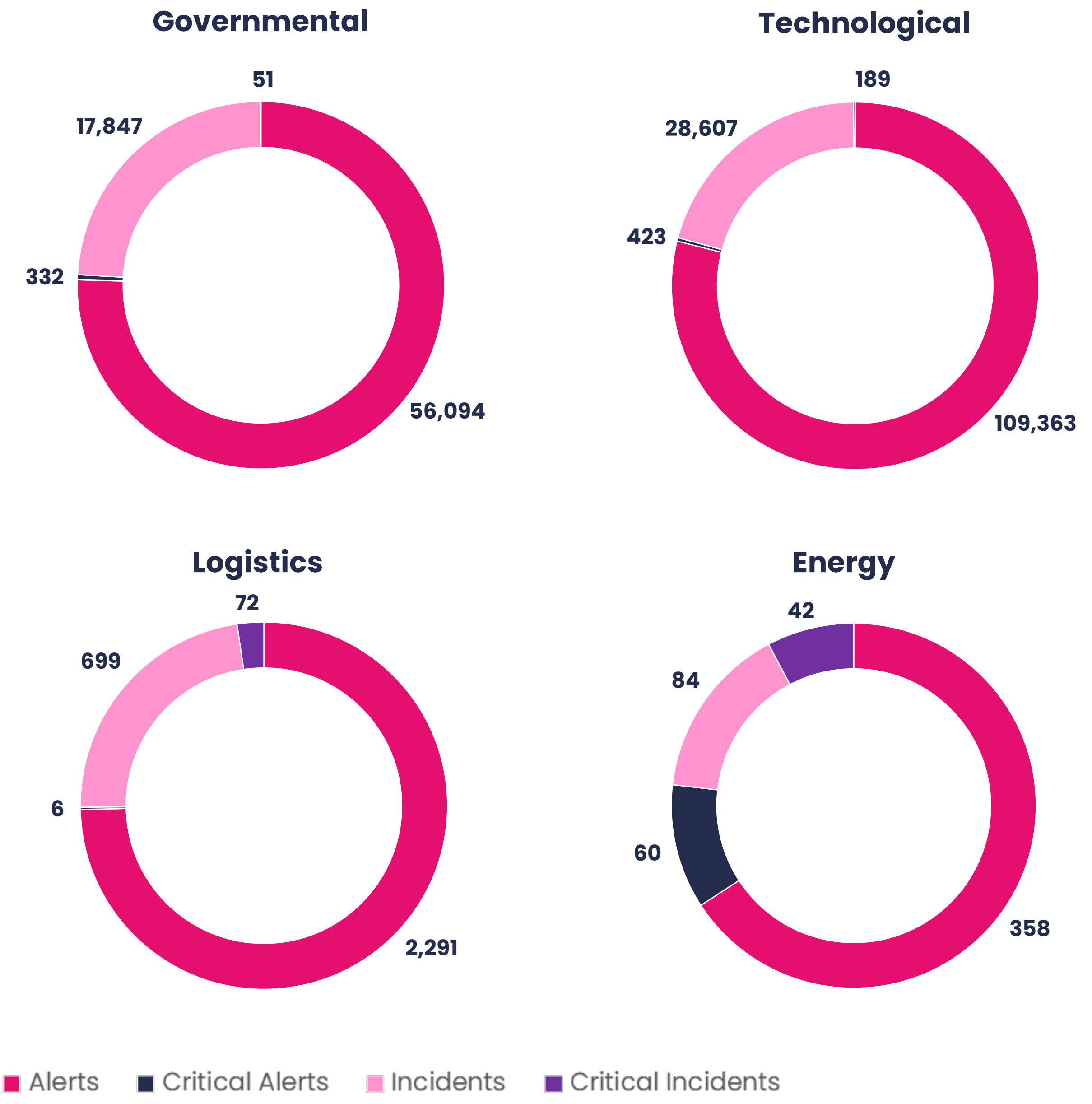
LAZARUS, CONTI, APT41 & APT29

2.1 Identified alerts and security incidents

Inetum's SOC managed a total of 169,788 security alerts for its customers in 2024. It also analysed 48,343 security incidents, providing information on their occurrence and mitigation. Of the alerts and incidents managed by the SOC, it is possible to establish a relationship between these and the sector to which these customers belong.

Regarding internal information on the number of alerts and incidents, the technology and government sectors stand out, as well as the logistics and energy sectors. It should be noted that the number of alerts and incidents is related to the number of Inetum SOC clients in each sector.

Table 1.
Number of internal incidents and alerts by sector



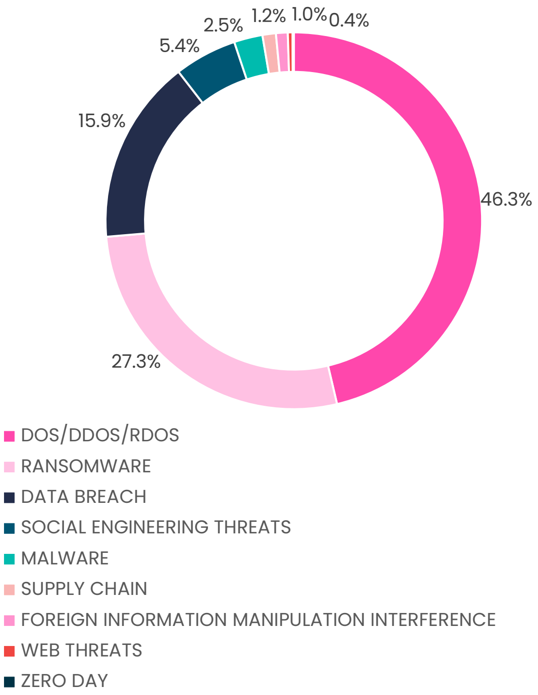
Source: Internal data. Own elaboration

03

Main Threats

ENISA, one of the most notorious sources of information on European threats, identifies DOS/DDOS/RDOS, Ransomware and data breaches as the most important threats in 2024

Table 2.
Percentage by threat groups in the EU



Source: ENISA Threat Landscape 2024. Own elaboration.

Also, from Inetum's SOC through the analysis of alerts and incidents identified for clients, the ten most common threats are established:

- **Internal SPAM distribution**
  Internal SPAM distribution can be a sign that an account within the organization has been compromised. This type of activity can be used to spread malware or phishing links.
- **External phishing campaigns**
  External phishing campaigns are one of the most common and dangerous cyber threats.
- **Suspicious host execution**
  Suspicious execution on a host may indicate the presence of malware or the activity of an attacker who has compromised the system.
- **Host with multiple infections**
  A host with multiple infections is a clear indication of a significant security breach.
- **Connections to domains with suspicious reputation**
  Connections to domains with suspicious reputations can be a sign that a device is attempting to communicate with attacker-controlled servers. These connections can facilitate malware downloads.
- **Suspicious detections on multiple hosts**
  Suspicious detections on multiple hosts suggest a coordinated attack or rapid malware spread.
- **Connections allowed to external domains**
  Allowing connections to external domains may be necessary for business operations but also represents a security risk.
- **External device infections on the same host**
  Infections of external devices on the same host indicate that a device, such as a USB drive, is compromised and spreads malware each time it is connected.
- **Active network scanning**
  Active network scanning is a technique used by attackers to identify vulnerabilities in the network infrastructure.
- **Possible brute force attack**
  A possible brute force attack involves repeated attempts to guess passwords to access systems or accounts.

3.1 DOS/DDOS/RDOS

This year, threat actor groups have used denial of service attacks (DOS, DDOS, RDOS). These groups are mainly related to ideological motivations, such as the Russia-related Noname057 group, which has targeted numerous Spanish public and private organizations.

NoName057

NoName057 is a pro-Russian hacktivist group that emerged in March 2022. NoName057 is believed to be sponsored or supported by the Russian nation-state, and its activities are often aligned with Russian interests.

They are known for conducting Distributed Denial of Service (DDoS) attacks against various targets, including government agencies, media, and private companies in Ukraine, the United States, and Europe.

3.2 Malware

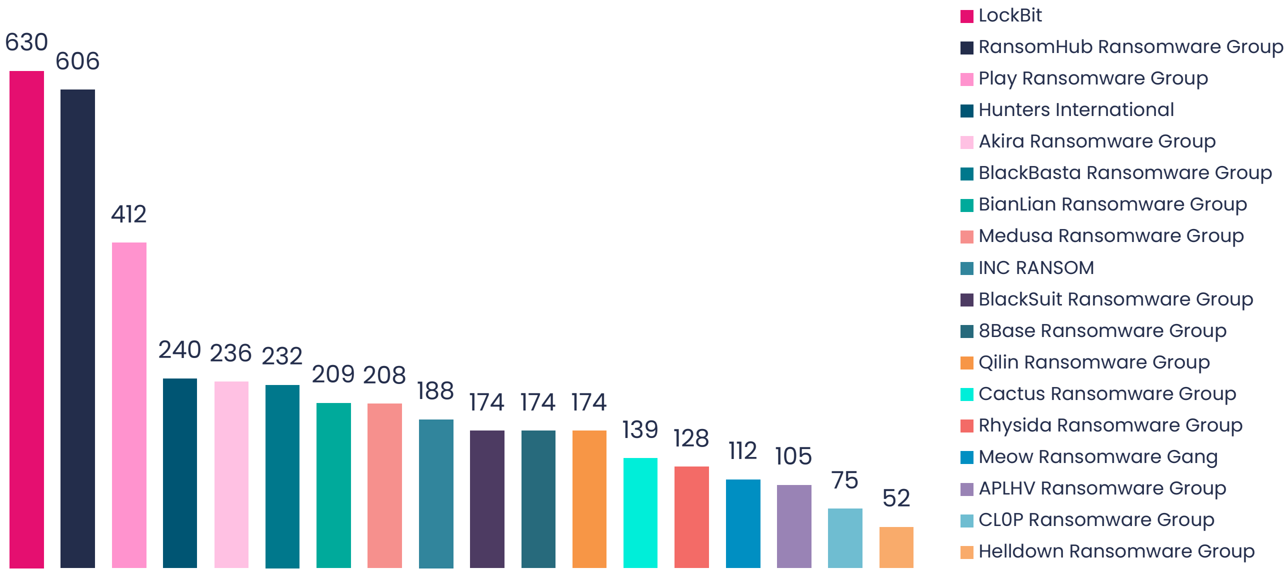
3.2.1 Ransomware

The increase in global ransomware attacks has particularly affected the industrial and manufacturing sectors, followed by retail and digital service providers. In Europe, ENISA has identified CLOP, LockBit, and 8BASE, among others, as the most active ransomware actors.

Internationally, in the analysis of more than 6,000 ransomware attacks collected by Recorded Future, LockBit, RansomHub, and Play Ransomware are identified as the most prolific actors.

Table 3.

Number of attacks by ransomware actors in 2024 at the international level



Source: Recorded Future. Own elaboration

To provide first-hand information about some of the most prominent actors and considering the sectors they target (prioritizing those that directly affect the sectors where SOC clients are located), the Threat Intelligence team has created customized reports. These reports analyze the actors, identify their tactics, techniques, and procedures, and disclose the associated Indicators of Compromise.

The actor reports produced by the Threat Intelligence team during 2024 are as follows:

Black Basta

- **In May 2024, an increase in attacks claimed by Black Basta was detected. Black Basta is a cybercriminal group operating under the Ransomware as a Service (RaaS) model, active since April 2022. There is evidence linking this group to FIN7 (Carbanak). Both groups have overlapping IP addresses used to communicate with Command and Control (C2) servers, employ similar attack techniques, and use EDR evasion techniques. Black Basta uses a double extortion method, demanding a ransom for decrypting systems under the threat of publishing exfiltrated data.**

BlackSuit

- **The threat actor known as BlackSuit has been operating since May 2023, targeting companies across various sectors, including healthcare, educational institutions, government agencies, construction, and industrial services. Investigations into its origin suggest it may be a new ransomware variant developed by the Royal group, a splinter of the defunct Conti group. There are operational similarities between BlackSuit and the Royal group. Both use similar open-source tools such as Chisel, Cloudflared, Secure Shell (SSH) Client, MobaXterm for establishing SSH connections, Mimikatz for credential theft, and Nirsoft for password collection.**

Meow Ransomware

- **The threat actor Meow ransomware, also known as "Meowcorp" or "Meowleaks," has been active since August 2022, primarily targeting the healthcare, education, industry, commerce, and government sectors. This group employs a variant of the Conti ransomware, focusing its attacks mainly on the United States, the United Kingdom, Colombia, Australia, and Spain. Meow ransomware poses a significant risk due to its sophisticated attack methods, which include phishing for initial access and the use of custom Python scripts for discovery and lateral movement within networks. Meow ransomware adds the ".MEOW" extension to encrypted files, making them easily identifiable.**

Volt Typhoon

- **The threat actor known as Volt Typhoon, also known as "BRONZE SILHOUETTE" or "Vanguard Panda," has been active since at least 2021 and has targeted organizations in critical sectors such as communications, manufacturing, media, defense, education, utilities, software and technology, transportation, construction, and government. This group is believed to operate under the direction of the Chinese government, reflecting a high level of organization and alignment with geopolitical objectives. Volt Typhoon represents a significant threat due to its sophisticated attack methods, which include exploiting known and zero-day vulnerabilities for initial access and leveraging advanced techniques such as "Living Off The Land" (LOTL) and credential harvesting for lateral movement. The group is highly skilled at maintaining stealth, using legitimate tools like PowerShell and exploiting Active Directory (AD) data to avoid detection while gaining full network access**

The Threat Hunting team works closely with the Threat Intelligence team, as Intelligence serves as the starting point for Hunting activities. This includes information on tactics, techniques, and procedures (TTPs) used by threat actors, as well as data on recent campaigns in the global cybersecurity environment.

In this context, the dedicated Threat Hunting team at INETUM's SOC conducts a proactive and continuous process aimed at identifying signs of malicious activity in the IT infrastructure, both in real-time and historical logs.

The threat actors for whom Threat Hunting reports have been produced during 2024 are:

Table 4.
Threat Huntings conducted in 2024

Phobos	Ransomhub	Akira
8base	BianLian	Medusa
Meow	BlackCat	Trigona
Helldown	Volt Thypoon	

Source: Internal data. Own elaboration

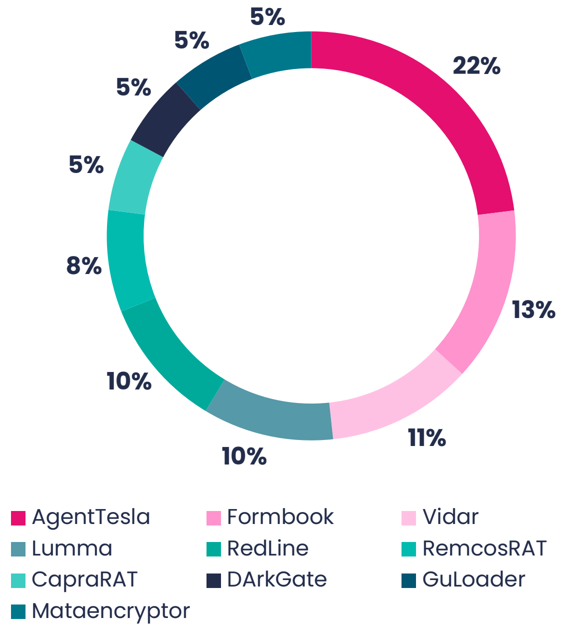
To understand the choice of these actors, it is useful to bear in mind that the development of previous Threat Hunting reports is based on three main pillars:

- **Hypothesis Definition:** Threat Hunting begins with the formulation of hypotheses based on Threat Intelligence, risk analysis, or anomalies detected in the infrastructure. These hypotheses are usually twofold and can be oriented towards investigating specific activities, such as recent indicators of compromise (reactive hunting) or active threats with a high probability of attacking the client based on their sector, the use of advanced exploitation tools, lateral movements, or unusual behaviors in users or systems (proactive hunting).
- **Data Collection and Analysis:** Relevant data is collected from multiple sources, such as logs, endpoint telemetry, network traffic, and detection platforms. Advanced tools like SIEMs (Security Information and Event Management systems) and EDRs (Endpoint Detection and Response) are used to identify suspicious patterns.
- Threat Identification: Through deep analysis and data correlation, indicators of malicious activity or behaviors that deviate from the norm are detected. This includes both known threats and new attack vectors that exploit undocumented vulnerabilities.

3.2.2 RATs & Stealers

The year 2024 has been characterized by the high activity of RATs[2] (Remote Access Trojans) and Stealers. Stealers, designed to steal sensitive information such as credentials and financial data, have seen an increase in use, possibly due to their effectiveness in phishing campaigns and other targeted attacks.

Table 5.
Number of RATs and Stealers attacks



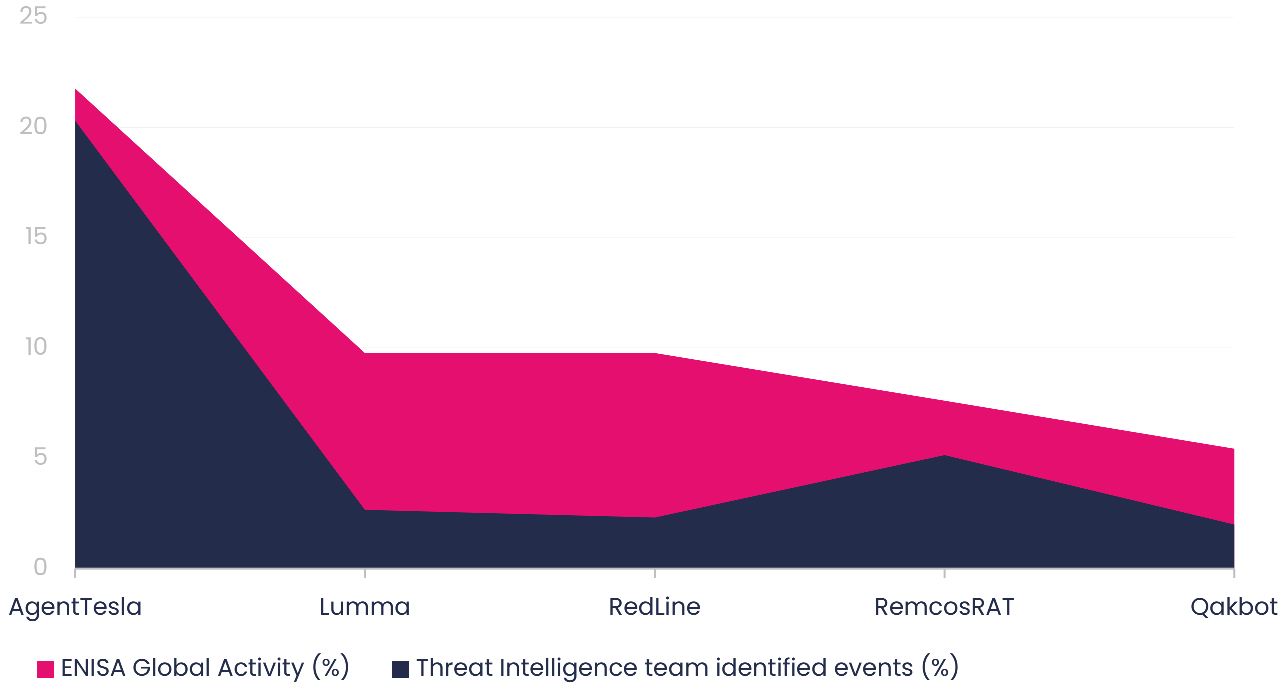
Source: ENISA Threat Landscape 2024. Own elaboration

[2] A Remote Access Trojan (RAT) is a type of malware used to gain complete access and remotely control a user's system, including their keyboard and mouse, access to their files, and network resources. The RAT gives attackers full control of a mobile or desktop device, allowing them to stealthily explore applications and files, and evade normal security measures such as firewalls, intrusion detection systems, and authentication controls.

On the other hand, RATs have allowed attackers to maintain remote control over compromised systems, facilitating espionage, data theft, and the execution of malicious commands. This increase is reflected in the number of events and indicators of compromise identified by the Threat Intelligence team during 2024.

Table 6.

Annual comparison of percentage by type of RAT and Stealer activity identified by ENISA vs. activity identified by the Threat Intelligence team



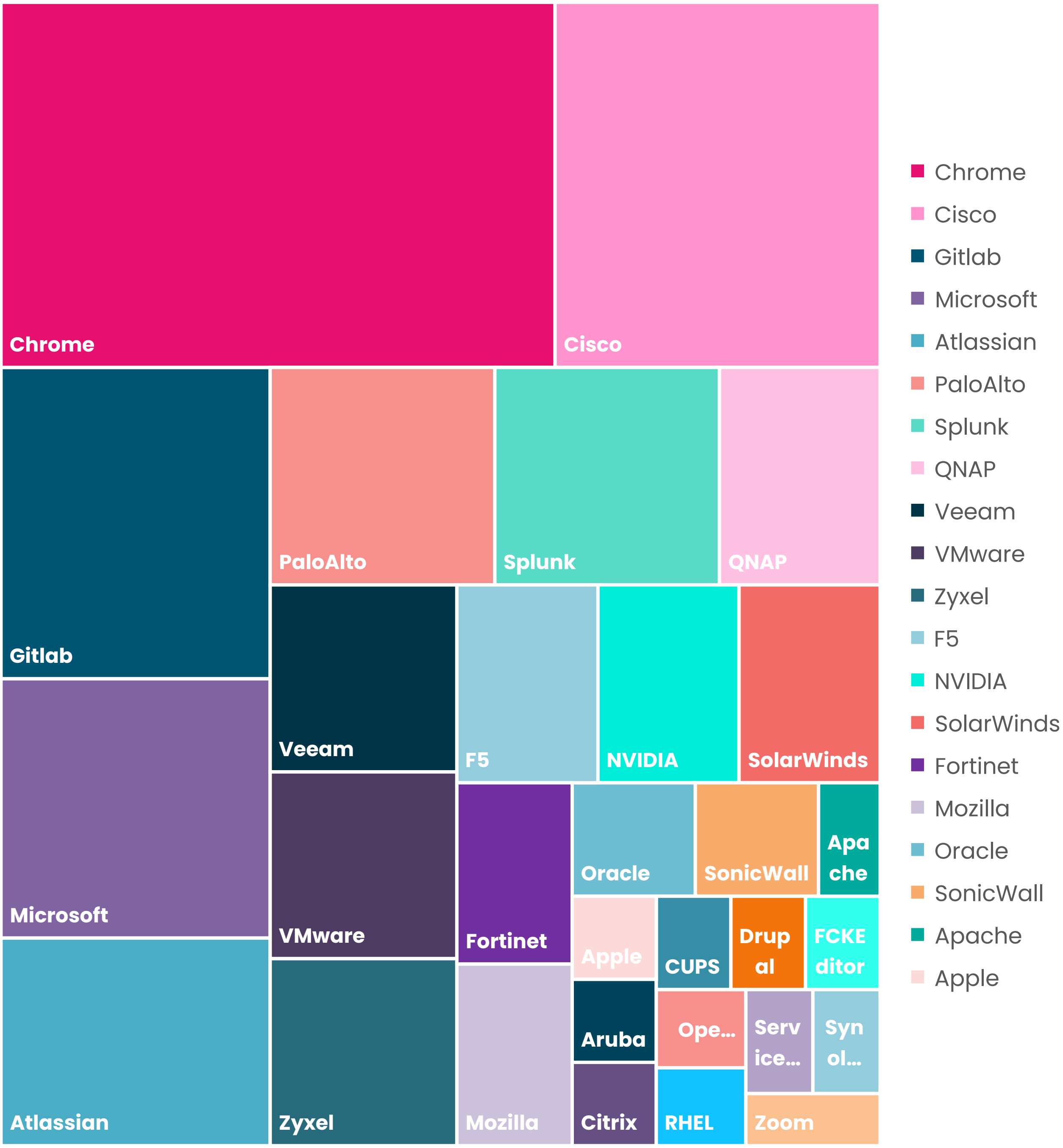
Source: Internal data and ENISA Threat Landscape 2024. Own elaboration

3.3 Vulnerabilities

Exploitation of vulnerabilities is one of the major threats this year. The Threat Intelligence team monitors alerts published by the main providers used by SOC clients. These vulnerabilities are reported after analyzing their impact, criticality, and mitigation, to alert about their publication and provide solutions to reduce their potential impact.

The following graph shows the number of investigations and reports conducted by each monitored technology provider:

Table 7.
Number of deliverables per technology



Source: Internal data. Own elaboration

3.3.1 Zero-days

Zero-days are vulnerabilities unknown to technology providers and without a patch or mitigation available at the time of their disclosure, allowing malicious actors to exploit them freely. The most impactful zero-days discovered in 2024 are as follows:

- **CVE-2024-56789, Adobe (Adobe Acrobat Reader)**
  Discovery date: March 15, 2024. This critical vulnerability allows for arbitrary code execution, memory leak, and denial of service in versions prior to 24.005.20307 of Adobe Acrobat and Reader. An attacker can exploit this vulnerability by creating a specially crafted PDF file that, when opened, executes malicious code on the victim's system.

- **CVE-2024-20353 y CVE-2024-20359, Cisco (ASA & FTD)**
  Discovery date: April 24, 2024. These vulnerabilities were exploited in the ArcaneDoor campaign. CVE-2024-20353 allows for a denial of service on Cisco ASA and FTD devices, disrupting their normal operation. CVE-2024-20359 enables persistent code execution on these devices, which can be used by an attacker to maintain unauthorized access and execute arbitrary commands.

- **CVE-2024-78901, VMware (vSphere)**
  Discovery date: June 10, 2024. A vulnerability in VMware vCenter allows for remote code execution due to memory management issues. It affects versions prior to those listed in VMSA-2024-0019. An attacker can send malicious requests to the vCenter server, potentially resulting in arbitrary code execution with the privileges of the vCenter service.

- **CVE-2024-89012, Google (Chrome)**
  Discovery date: July 5, 2024. The vulnerability involves type confusion in the V8 engine of Chrome, allowing a remote attacker to exploit memory corruption through a specially crafted HTML page. This can lead to arbitrary code execution within the browser context, enabling the attacker to take control of the affected system.

- **CVE-2024-23456, Zscaler (Client Connector)**
  Discovery date: August 6, 2024. This vulnerability allows an attacker to disable tamper protection in Zscaler Client Connector in versions prior to 4.2.0.190 without signature validation. This means an attacker can modify the client's configuration undetected, potentially leading to the deactivation of critical security measures.

- **CVE-2024-12345, GitLab (CE/EE)**
  Discovery date: August 7, 2024. A critical vulnerability in the management of authentication tokens allows an unauthenticated attacker to assign administrative privileges, granting them full control over the affected GitLab instance. This vulnerability can be exploited remotely without prior compromise.

- **CVE-2024-90123, Microsoft (Windows)**
  Discovery date: September 18, 2024. This critical remote code execution vulnerability affects multiple versions of Windows Server. It allows attackers to execute arbitrary code remotely, potentially granting them full control over the affected system. Exploitation can be achieved by sending specially crafted packets to a vulnerable server.

04

Tactics and Techniques

Based on the analysis of RATs and Stealers detailed in section 3.2.2, the following Techniques, Tactics, and Procedures are particularly noteworthy[3]:

Initial Access

T1566: Phishing - Adversaries can send phishing messages to gain access to victims' systems. All forms of phishing are social engineering delivered electronically. Phishing can be targeted, known as spearphishing. In spearphishing, the adversary targets a specific person, company, or sector. More generally, adversaries can conduct untargeted phishing, such as in mass spam campaigns.

T1566.001: Spearphishing Attachment - Adversaries can send spearphishing emails with a malicious attachment to access victims' systems. Spearphishing with an attachment is a specific variant of spearphishing. It differs from other forms of spearphishing by using malware attached to an email. All forms of spearphishing are social engineering delivered electronically and targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and generally rely on user execution to achieve their goal. Spearphishing can also involve social engineering techniques, such as impersonating a trusted source.

T1566.002: Spearphishing Link - Adversaries can send spearphishing emails with a malicious link in an attempt to access victims' systems. Spearphishing with a link is a specific variant of spearphishing. It differs from other forms of spearphishing by using links to download malware contained in the email, rather than attaching malicious files directly to the email, to avoid defenses that may inspect attachments. Spearphishing can also involve social engineering techniques, such as impersonating a trusted source.

Execution

T1059: Command and Scripting Interpreter - Adversaries can abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways to interact with computer systems and are a common feature across many different platforms.

T1106: Native API - Adversaries can interact with the native application programming interface (API) of the operating system to execute behaviors. Native APIs provide a controlled means to call low-level operating system services within the kernel, such as those involving hardware/devices, memory, and processes. These native APIs are utilized by the operating system during system boot (when other system components are not yet initialized) as well as to perform tasks and requests during routine operations.

[3] MITRE ATT&CK Framework v16.

T1204.002: Malicious File - An adversary may rely on a user opening a malicious file to achieve execution. Users can be subjected to social engineering techniques to open a file that will lead to code execution. This user action is typically observed as a follow-up behavior to spearphishing with an attachment.

Persistence

T1547.001: Registry Run Keys / Startup Folder - Adversaries can achieve persistence by adding a program to a startup folder or referencing it with a run key in the Registry. Adding an entry to the 'run keys' in the Registry or the startup folder will cause the referenced program to execute when a user logs in. These programs will run under the user's context and have the permission level associated with the account.

Privilege Escalation

T1055: Process Injection - Adversaries can inject code into processes to evade process-based defenses and possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Executing code in the context of another process can allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution through process injection can also evade detection by security products, as the execution is masked under a legitimate process.

Defense Evasion

T1562: Impair Defenses - Adversaries can maliciously modify components of a victim's environment to hinder or disable defense mechanisms. This not only involves impairing preventive defenses, such as firewalls and antivirus software, but also the detection capabilities that defenders use to audit activity and identify malicious behavior. This can encompass both native defenses and supplementary capabilities installed by users and administrators.

T1027: Obfuscated Files or Information - Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or obfuscating its content on the system or in transit. This is a common behavior that can be used across different platforms and networks to evade defenses.

T1497: Virtualizaction / Sandbox Evasion - Adversaries may employ various methods to detect and avoid virtualization and analysis environments. This can include altering behaviors based on the results of checks for artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may modify their malware to disconnect from the victim or hide the main functions of the implant. They may also look for VME artifacts before deploying secondary or additional payloads.

Credential Access

T1056: Input Capture - Adversaries can use user input capture methods to obtain credentials or gather information. During normal system use, users often provide credentials in various places, such as login pages/portals or system dialog boxes. Input capture mechanisms can be transparent to the user or rely on tricking the user into providing information in what they believe is a genuine service.

Discover

T1057: Process Discovery - Adversaries may attempt to gather information about running processes on a system. The information obtained could be used to understand common software/applications running on systems within the network. Administrator or other elevated access can provide better details of the processes. Adversaries may use the information from Process Discovery during automated discovery to shape subsequent behaviors, including whether the adversary fully infects the target and/or attempts specific actions.

Collection

T1056.001: Keylogging - Adversaries can log a user's keystrokes to intercept credentials as the user types them. Keystroke logging is likely used to acquire credentials for new access opportunities when operating system credential dumping efforts are ineffective. It may require an adversary to intercept keystrokes on a system for a substantial period before credentials can be successfully captured. To increase the likelihood of quickly capturing credentials, an adversary may also take actions such as clearing browser cookies to force users to re-authenticate on systems.

Command and Control

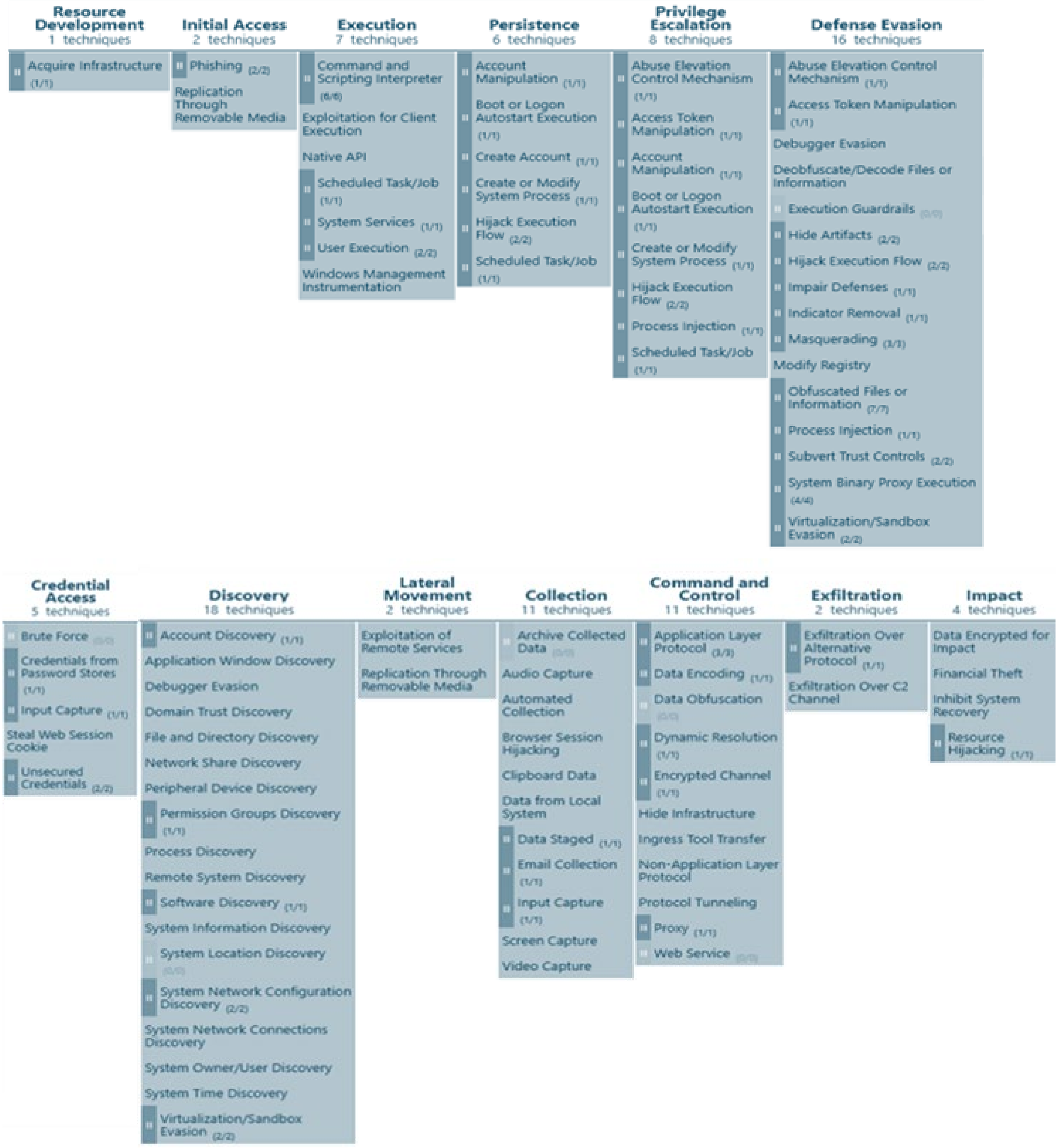
T1071: Application Layer Protocol - Adversaries can communicate using application layer protocols of the OSI model to avoid detection or network filtering by blending with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and the server.

T1105: Ingress Tool Transfer - Adversaries can transfer tools or other files from an external system to a compromised environment. Tools or files can be copied from a system controlled by the external adversary to the victim's network via the command and control channel or through alternative protocols such as FTP. Once present, adversaries can also transfer/distribute tools among the victim's devices within a compromised environment.

The complete list of TTPs can be found in the following image:

Table 8.

MITRE ATT&CK Enterprise v16 – Overlapping techniques for analysed malware



Resource Development 1 techniques	Initial Access 2 techniques	Execution 7 techniques	Persistence 6 techniques	Privilege Escalation 8 techniques	Defense Evasion 16 techniques
Acquire Infrastructure (1/1)	Phishing (2/2)	Command and Scripting Interpreter (6/6)	Account Manipulation (1/1)	Abuse Elevation Control Mechanism (1/1)	Abuse Elevation Control Mechanism (1/1)
	Replication Through Removable Media	Exploitation for Client Execution	Boot or Logon Autostart Execution (1/1)	Access Token Manipulation (1/1)	Access Token Manipulation (1/1)
		Native API	Create Account (1/1)	Account Manipulation (1/1)	Debugger Evasion
		Scheduled Task/Job (1/1)	Create or Modify System Process (1/1)	Boot or Logon Autostart Execution (1/1)	Deobfuscate/Decode Files or Information
		System Services (1/1)	Hijack Execution Flow (2/2)	Create or Modify System Process (1/1)	Execution Guardrails (0/0)
		User Execution (2/2)	Scheduled Task/Job (1/1)	Hijack Execution Flow (2/2)	Hide Artifacts (2/2)
		Windows Management Instrumentation		Process Injection (1/1)	Hijack Execution Flow (2/2)
				Scheduled Task/Job (1/1)	Impair Defenses (1/1)
					Indicator Removal (1/1)
					Masquerading (3/3)
					Modify Registry
					Obfuscated Files or Information (7/7)
					Process Injection (1/1)
					Subvert Trust Controls (2/2)
					System Binary Proxy Execution (4/4)
					Virtualization/Sandbox Evasion (2/2)

Credential Access 5 techniques	Discovery 18 techniques	Lateral Movement 2 techniques	Collection 11 techniques	Command and Control 11 techniques	Exfiltration 2 techniques	Impact 4 techniques
Brute Force (0/0)	Account Discovery (1/1)	Exploitation of Remote Services	Archive Collected Data (0/0)	Application Layer Protocol (3/3)	Exfiltration Over Alternative Protocol (1/1)	Data Encrypted for Impact
Credentials from Password Stores (1/1)	Application Window Discovery	Replication Through Removable Media	Audio Capture	Data Encoding (1/1)	Exfiltration Over C2 Channel	Financial Theft
Input Capture (1/1)	Debugger Evasion		Automated Collection	Data Obfuscation (0/0)		Inhibit System Recovery
Steal Web Session Cookie	Domain Trust Discovery		Browser Session Hijacking	Dynamic Resolution (1/1)		Resource Hijacking (1/1)
Unsecured Credentials (2/2)	File and Directory Discovery		Clipboard Data	Encrypted Channel (1/1)		
	Network Share Discovery		Data from Local System	Hide Infrastructure		
	Peripheral Device Discovery		Data Staged (1/1)	Ingress Tool Transfer		
	Permission Groups Discovery (1/1)		Email Collection (1/1)	Non-Application Layer Protocol		
	Process Discovery		Input Capture (1/1)	Protocol Tunneling		
	Remote System Discovery		Screen Capture	Proxy (1/1)		
	Software Discovery (1/1)		Video Capture	Web Service (0/0)		
	System Information Discovery					
	System Location Discovery (0/0)					
	System Network Configuration Discovery (2/2)					
	System Network Connections Discovery					
	System Owner/User Discovery					
	System Time Discovery					
	Virtualization/Sandbox Evasion (2/2)					

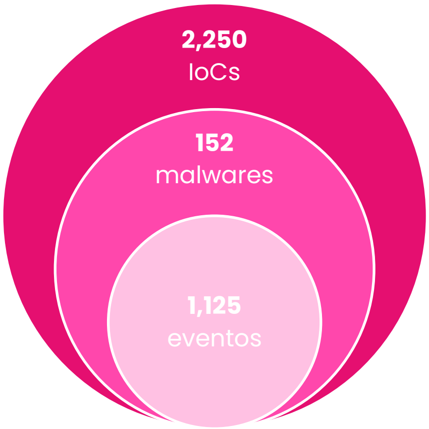
Source: Internal data. Own elaboration

05 Indicators of Compromise

Indicators of Compromise (IoCs) help cybersecurity analysts identify malicious activities or security threats, such as data breaches, insider threats, or malware attacks. IoCs can be very diverse and vary depending on the malicious activity, including IPs, URLs, domains, hashes, etc.

The Threat Intelligence team at the SOC reviews potential IoCs to feed the various detection systems that serve the function of protecting clients. In 2024, a total of 2,250 indicators of compromise were shared. These indicators are distributed across 1,125 events[4].

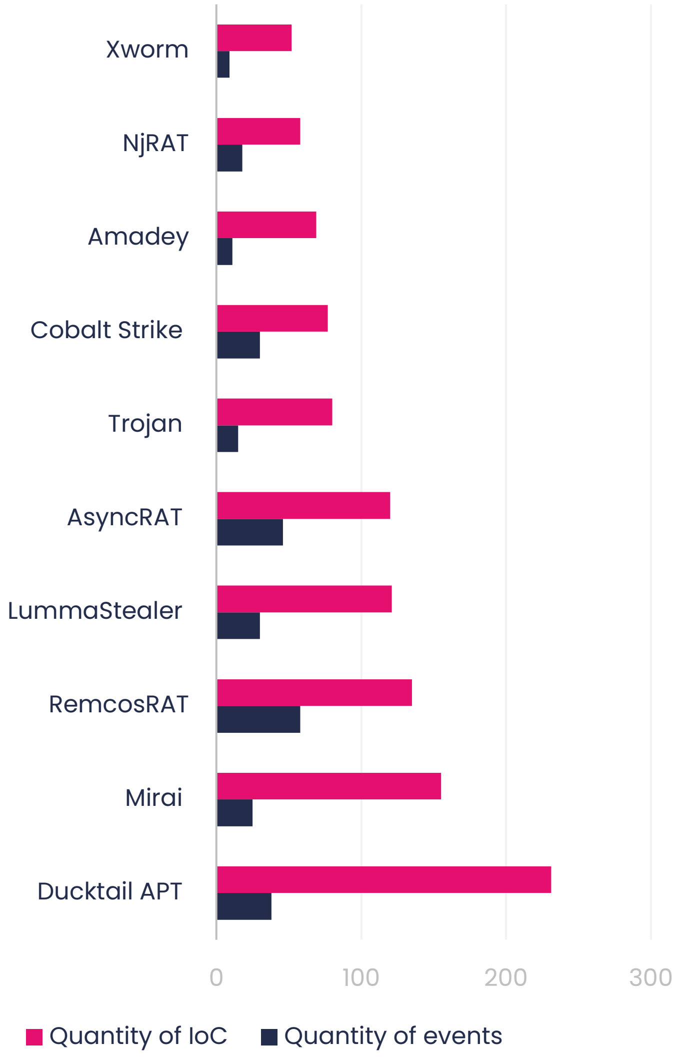
Table 9.
Number of IoCs identified, malware, and events



Source: Internal data. Own elaboration

From the indicators of compromise and the events created, 152 different types of malware have been identified, including the following notable ones:

Table 10.
Relationship between the number of events and IoCs



Source: Internal data. Own elaboration

[4] The word events is part of the nomenclature used by the National Security Network, these events could be considered as sets of indicators of compromise that are related to each other, by the characteristics of malware, associated files, executables, among others, and that are related in time. In the case of events related to malicious actors, these can be considered as attack campaigns.

In the global cybersecurity landscape, collaboration between technology consultancies and key entities is essential for defending against cyber threats. Technology consultants are crucial in strengthening cybersecurity at both national and international levels. Participation in collaborative networks allows for contributions to the development of innovative solutions and the implementation of advanced defense strategies. This approach addresses an increasingly dynamic threat environment.

MISP

MISP (Malware Information Sharing Platform & Threat Sharing) is an open-source platform designed for the collection, storage, and sharing of cybersecurity indicators and threats related to security incidents and malware analysis. It facilitates collaboration between organizations by sharing structured threat information, thereby improving the detection and response to cyberattacks.

The Threat Intelligence team uses the platform to perform tasks such as feeding, collecting, validating, and pre-analyzing indicators of compromise, as well as systematically integrating data from various internal and external sources. This process ensures that the platform is constantly updated with accurate and relevant information, enhancing the ability to identify patterns, anticipate risks, and coordinate responses effectively in an ever-evolving threat environment.

SOC National Network

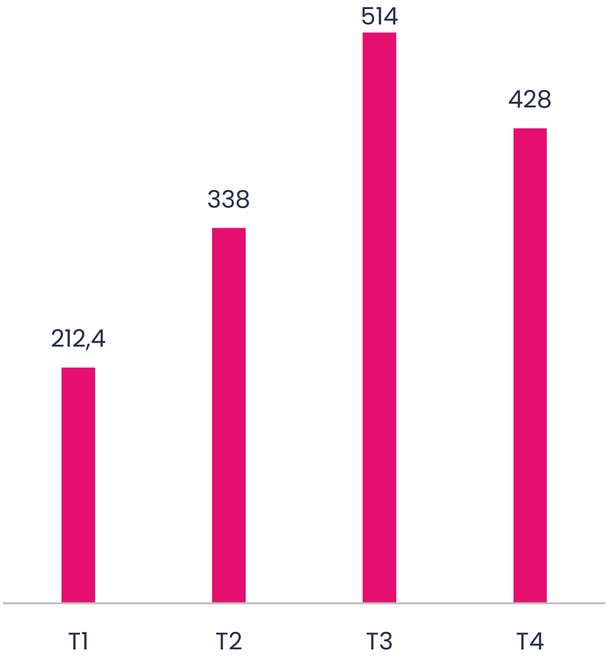
From Inetum's SOC, there is an active collaboration with the SOC National Network (RNS).

This platform was created by the National Cryptologic Center (CCN-CERT) to coordinate collaboration and information exchange between Cybersecurity Operations Centers (SOCs) in Spain, both public and private.

The main objective of the RNS is to improve protection against cyber threats through early detection and almost immediate blocking of any anomalous activity detected at any point in the administration. This is achieved by sharing information about tactics, techniques, and procedures of new threats among the SOCs, allowing for a faster and more effective response to potential cyber incidents [5].

It is worth noting the **Gold level of participation achieved by Inetum**. The number of IoCs shared, and therefore Inetum's participation in the RNS, has improved in 2024 compared to 2023 according to official data provided by the organization.

Table 11.
Relationship of IoCs shared in the RNS by quarter



Source: Official data from the SOC National Network. Own elaboration

[5] Information about RNS: https://rns.ccn-cert.cni.es/

FIRST

Inetum continuously collaborates with incident response teams worldwide, strengthening global cybersecurity. Through entities like FIRST, technology consultancies contribute to the development of international cybersecurity standards and share their expertise in managing complex incidents. This helps establish a common framework for effectively responding to threats.

Collaboration allows access to a global network of experts, providing a strategic advantage by staying informed about emerging threats and practices at an international level. The shared information on vulnerabilities, attack techniques, and emerging threats facilitates a more effective response to cyber risks worldwide.

CSIRT Spain

Inetum strengthens the protection of critical infrastructures and the management of cyber incidents. It actively participates in the development of advanced tools for cybersecurity management, including the integration of emerging technologies such as artificial intelligence and big data analytics. In this regard, technology consultancies contribute to the development and refinement of advanced tools for incident management.

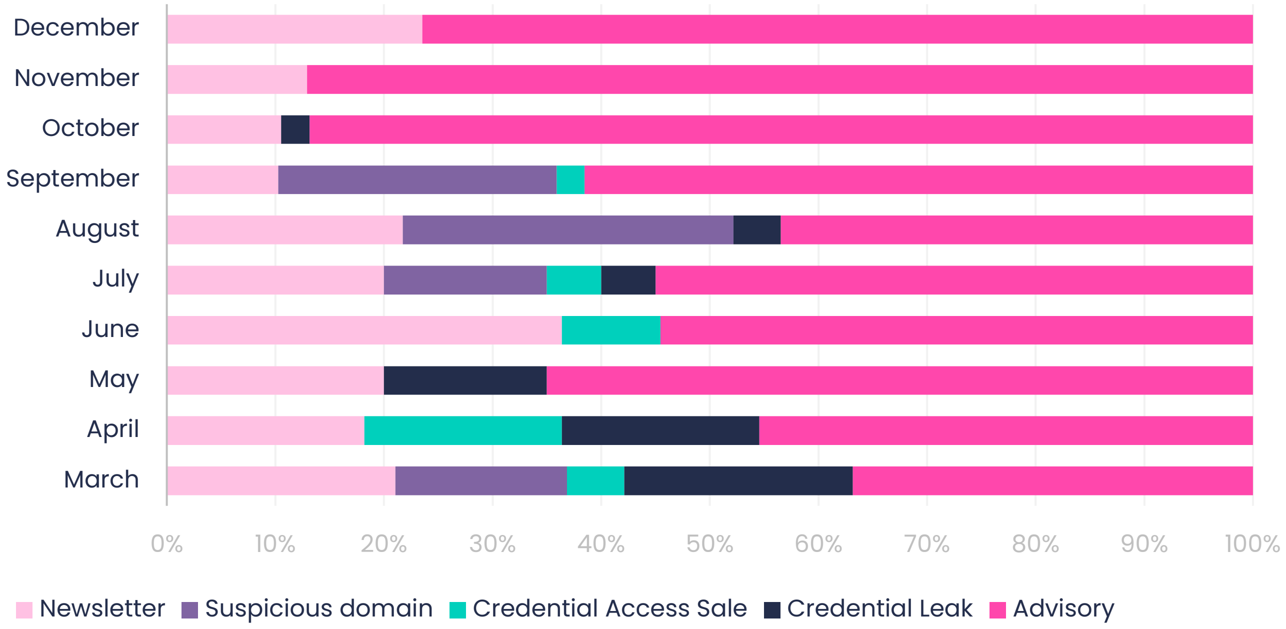
The implementation of innovative technologies like artificial intelligence and big data analytics enhances the CSIRT's ability to detect and mitigate threats more quickly and accurately. Additionally, consultants actively collaborate in the continuous training and education of CSIRT personnel, ensuring they are always prepared to face emerging challenges in cyberspace. Thus, consultancies establish themselves as strategic partners in the protection of critical infrastructures and the country's digital security.

06
Deliverables

In the Threat Intelligence team of the SOC, clients are provided with up-to-date information on alerts and security warnings from technology providers, as well as a weekly newsletter that compiles alerts, active campaigns, and news. Additionally, monitoring is conducted on open sources, the Dark Web, and the Deep Web for assets of various clients who have contracted this service, in order to notify them of suspicious domains, sale of access and credentials, and leaks from their organizations.

Table 12.

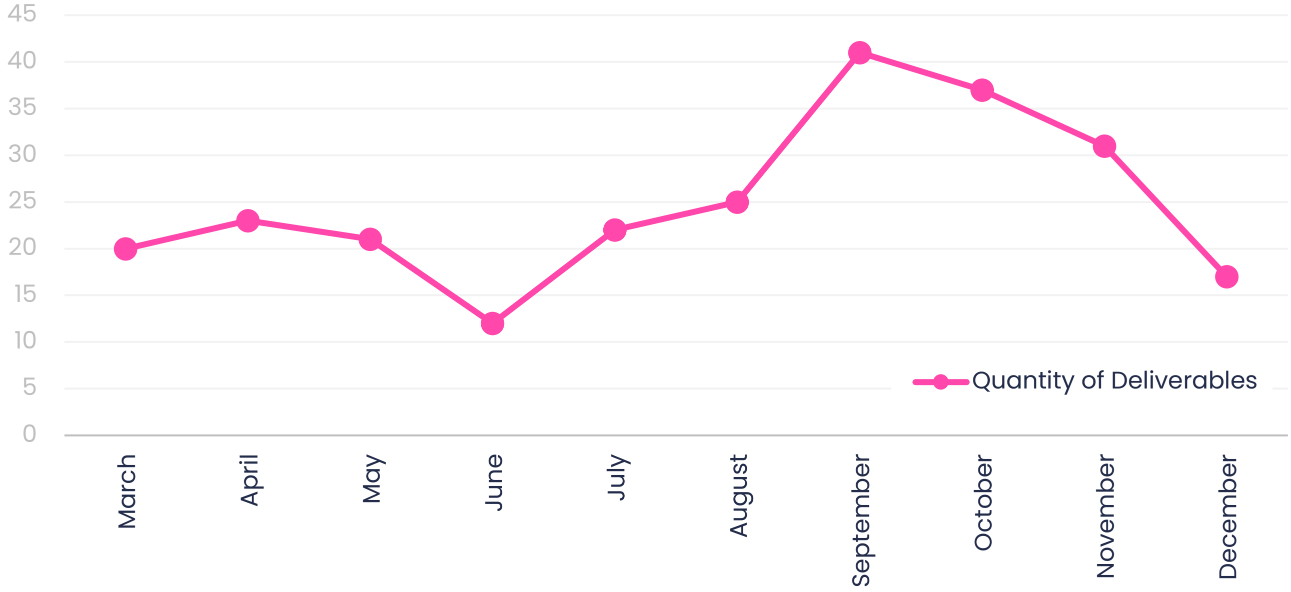
Number of reports by type



Source: Internal data. Own elaboration

Table 13.

Total number of reports per month



Source: Internal data. Own elaboration

Timeline of deliverables

JANUARY
11 Alerts
4 Newsletters
1 Report

FEBRUARY
9 Alerts
4 Newsletters
1 Report

MARCH
7 Alerts
4 Newsletters
1 Report
7 Investigations

APRIL
8 Alerts
4 Newsletters
2 Reports
8 Investigations

MAY
11 Alerts
4 Newsletters
3 Reports
2 Investigations

JUNE
4 Alerts
4 Newsletters
2 Reports
2 Investigations

JULY
9 Alerts
4 Newsletters
4 Reports
4 Investigations

AUGUST
8 Alerts
4 Newsletters
7 Reports
3 Investigations

SEPTEMBER
18 Alerts
4 Newsletters
7 Reports
11 Investigations

OCTOBER
24 Alerts
4 Newsletters
7 Reports
2 Investigations

NOVEMBER
24 Alerts
4 Newsletters
1 Report
2 Investigations

DECEMBER
11 Alerts
4 Newsletters
2 Reports

07

Trends 2025

The international cybersecurity landscape is expected to continue experiencing an increase in the number of attacks, particularly targeting the government, technology, energy, and critical infrastructure sectors. Large companies are likely to be the most affected due to the nature of the most common attacks, such as denial-of-service (DoS) attacks and ransomware, which aim to cause the greatest possible impact and obtain significant economic benefits. The rapid evolution of attackers' tactics and the use of advanced technologies to evade traditional defenses will increase the complexity of the risks.

This threat environment will require a more robust response adapted to new challenges, making it essential to continuously strengthen cybersecurity capabilities in key sectors to protect both sensitive data and the critical operations of organizations in the country.

DOS/DDOS/RDOS

Denial-of-service attacks are expected to persist into the next year, influenced by the ongoing conflicts between Russia and Ukraine, as well as Iran and Israel. This trend will depend on the progression of these conflicts, with their severity and impact either increasing or decreasing. Consequently, the most prominent groups will be state-sponsored actors and hacktivists.

Ransomware

Ransomware groups increased their activity in 2024, and despite the efforts of law enforcement agencies to curb their operations, the emergence of new groups and the number of attacks suggest that the upward trend will continue through 2025.

The most notable technique for this type of threat in the coming year is session hijacking, using malware to capture session cookies and bypass multi-factor authentication (MFA).

Additionally, the Ransomware as a Service (RaaS) model, which allows cybercriminals without advanced technical skills to launch ransomware attacks, will continue to grow due to its ease of access and profitability.

RATs-Stealers

Remote Access Trojans (RATs) and Stealers (information thieves) will continue to evolve, becoming more automated and sophisticated, leveraging artificial intelligence to evade detection and enhance the effectiveness of attacks. IoT devices will remain one of their primary targets to compromise devices and gain access to much broader networks. Additionally, their use will continue to be integrated into phishing campaigns for the effective distribution of malware.

Vulnerabilities, Zero-days

An increase in the exploitation of zero-day vulnerabilities in the cloud is expected, as threat actors will focus their attention on these services due to their growing use. Additionally, artificial intelligence and machine learning will continue to be used to automate the identification and exploitation of vulnerabilities, increasing the speed and effectiveness of attacks. Zero-day exploits will continue to become more sophisticated, using advanced techniques to evade defenses and remain undetectable for longer periods.

Artificial Intelligence

Artificial Intelligence (AI) will continue to be a key tool for threat actors, automating the identification and exploitation of vulnerabilities, as well as the creation of malware and disinformation campaigns.

Attackers will leverage machine learning algorithms to increase the efficiency and impact of their operations, improving their ability to evade defenses and making detection more difficult. As AI advances, both offensively and defensively, attacks will become more sophisticated, adapting to and circumventing security measures, which will complicate their anticipation and mitigation.

inetum.

inetum.com