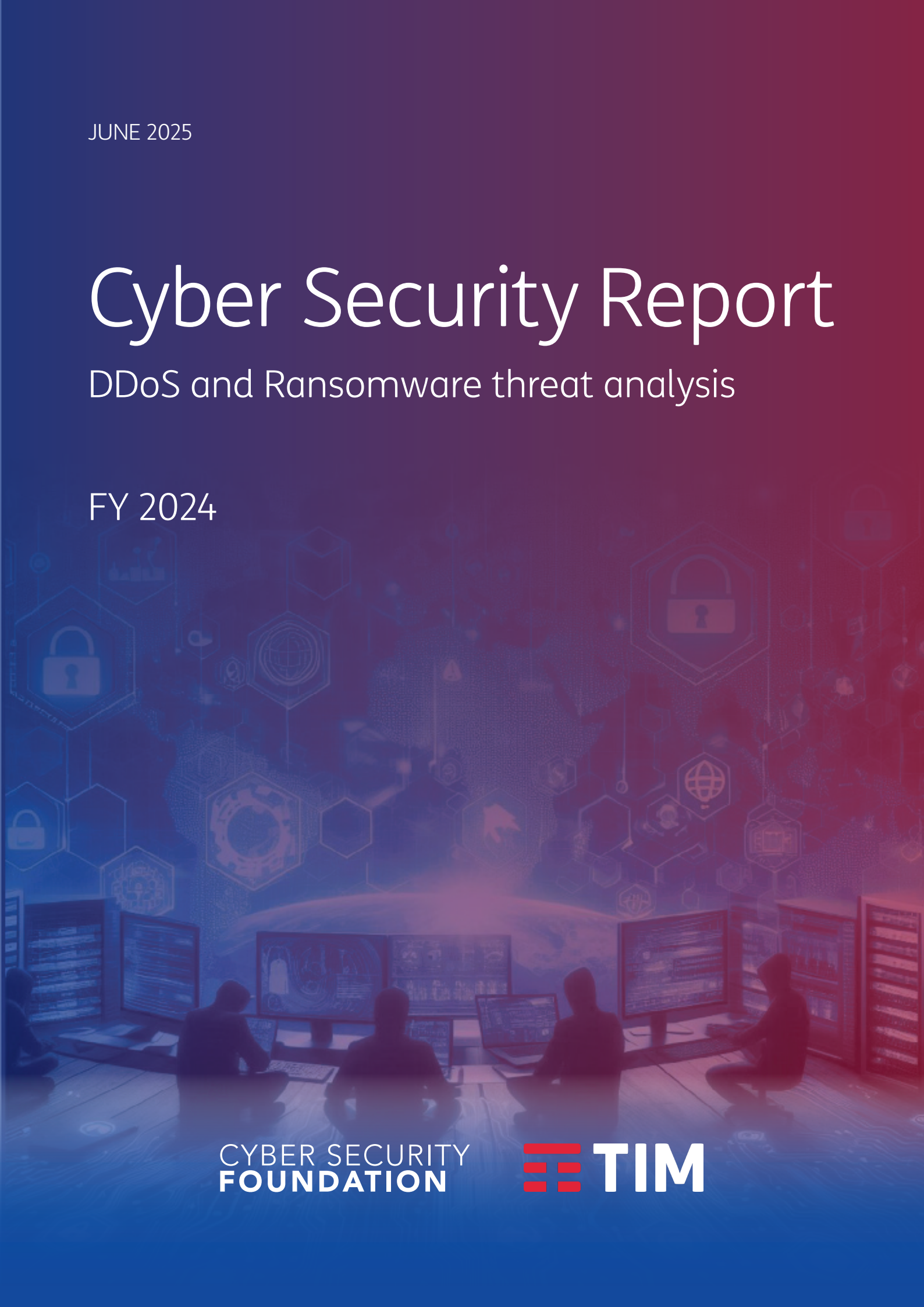
JUNE 2025

Cyber Security Report

DDoS and Ransomware threat analysis

FY 2024



CYBER SECURITY FOUNDATION

TIM

Executive Summary

1) About this report

As digitalisation spreads, the areas exposed to cyber threats increase. This concerns us all: institutions, businesses, ordinary citizens. No system is 100% safe, but it is possible to build a resilient system, based on a better knowledge on how these events occur. This report is produced by the Italian Cyber Security Foundation, whose mission is to deepen and spread the cyber security culture in Italy, and TIM, which carries out daily actions to prevent and mitigate cyber incidents through its CyberSOCs and other Group entities such as Telsy and TS-Way, and is divided into four specific areas:

- **Main attacks**: observation of the most relevant cyber events of the year, focusing on DDoS and Ransomware attacks, based on operational data gathered by TIM.
- **Sectoral analysis**: analysis of the attacks by sector, with a particular focus on the corporate, productive and institutional worlds, to identify the most affected areas and the main threat scopes.
- **Regulatory Developments**: overview on the strategies and regulatory initiatives at European and Community level, aimed to reinforce the cyber defence of the Union and its member States, among which Italy is included.
- **Emerging technologies**: focus on the technological innovations transforming cybersecurity, both from the defence and attack points of view.

2) Main Attacks

The first part of the report is focused on the security events detected during 2024 by TIM's cyber defence teams, especially by the Security Operation Center and the Threat Intelligence units. The aim is to distinguish between mere threats and real attacks, emphasizing the role of prevention and continuous monitoring.

2.1. DDoS - Distributed Denial of Service

DOS «Denial of Service» attacks are among the threats to assets/digital services availability, targeting servers, websites and infrastructures with massive traffic volumes, generating an overload that prevents the regular provision of services. These can be performed also by exploiting compromised devices or the networks of unsuspecting users, which the attacker is able to take control of. The aim is to saturate targets resources to the point of making them unusable. Although the dynamics of the attacks are known, their detection remains complex: they can develop slowly and in waves, come from multiple geographic areas or hide behind apparently legitimate traffic. Some attacks even target monitoring systems. Besides, the use of artificial intelligence by the aggressors makes the attacks even more sophisticated and difficult to detect.

Below is the most significant information for 2024, detected through the direct monitoring of the TIM Group SOCs networks.

DDoS attacks return to pandemic levels

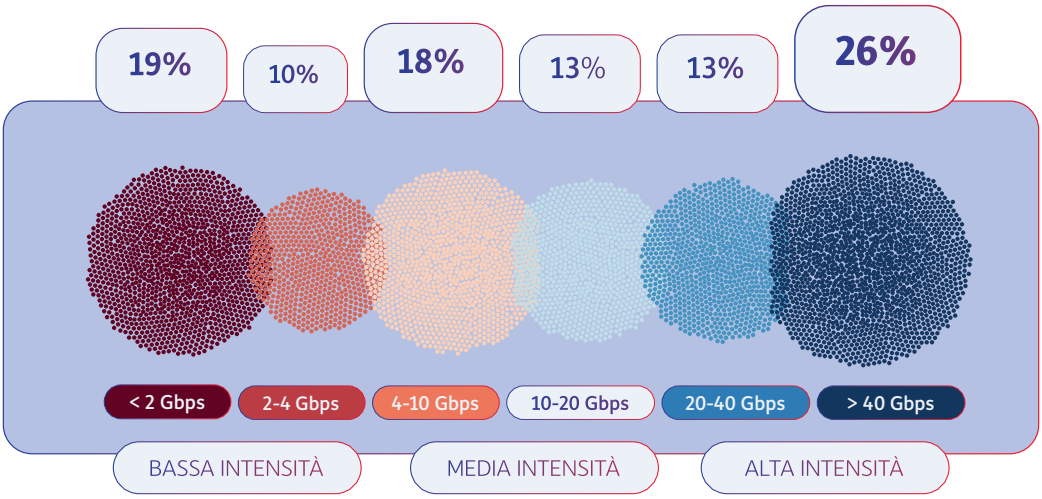
2024 registered a strong intensity in terms of DDoS events, with an increase of 36% compared to 2023: on average, there were around 560 cases per month with two peak moments and a progressive decrease in the last quarter of the year. From August 2023 to December 2024, an average of 580 cases per month emerged, with a peak of 765 events, which is similar to the levels of the pandemic period. The reasons behind the intensification of DDoS attacks are both financial and geopolitical in nature, related to the Ukrainian war and the Gaza strip conflict, worsening the overall situation.

New technologies and attack techniques are emerging

In 2023–2024, a rise in DDoS threats has been observed, with the adoption of increasingly sophisticated techniques: hyper-volumetric attacks, capable of generating hundreds of millions of requests per second; multi-vectors attacks, compromised IoT devices and virtual machines (VM/VPS) included, generating traffic up to 5,000 times higher compared to a single device; multi-target attacks, which simultaneously target websites, networks, devices and infrastructures of a single organisation, making many legacy defences ineffective. The attacks evolved also at application level. Attacks targeting Web interfaces and APIs are gradually being detected, as they are difficult to identify due to encrypted traffic. Some of the attacks target DNS, which, overloaded with massive requests, block the resolution of web addresses. Advanced elusive techniques are being used, such as dynamic IPs and manipulated HTTP headers, in order to mask malicious traffic. These diverse attack modes and techniques make the timely detection and the implementation of effective countermeasures ever more complex.

The attack intensity class increases

In 2024 nearly 6,700 DDoS events were detected, a volume equal to that of the second pandemic lockdown. These events are radically different in terms of intensity. In 2024, the events with intensity lower than 10 Gbps accounted for 47% of the total, compared to 80% in 2021. Conversely, the attacks exceeding 20 Gbps rose from 5% (2021) to 39% in 2024, with a peak of 26% above 40 Gbps, today the most relevant class (every 10 events, 4 are of high intensity). Although lower intensity attacks are no less dangerous (because they can hide within legitimate traffic), this change highlights an evident increase in the attackers' offensive capacity, requiring an adjustment in defensive countermeasures.



A second essential parameter: the duration of the attack

The intensity level of the attacks should be examined along with their duration. DDoS events may have different durations: minutes, hours or even days. In 2024 the average duration of a DDoS event was approximately 39 minutes. The categories of very long attacks, lasting over 24 hours, decrease compared to 2023 and are now rare and episodic, while DDoS events lasting between 30 min and 2 hours, and under 24 hours, are increasing. This trend is linked to greater broadband availability and use of innovative technologies such as AI and cloud computing.

Allocation of DDoS attacks per sector

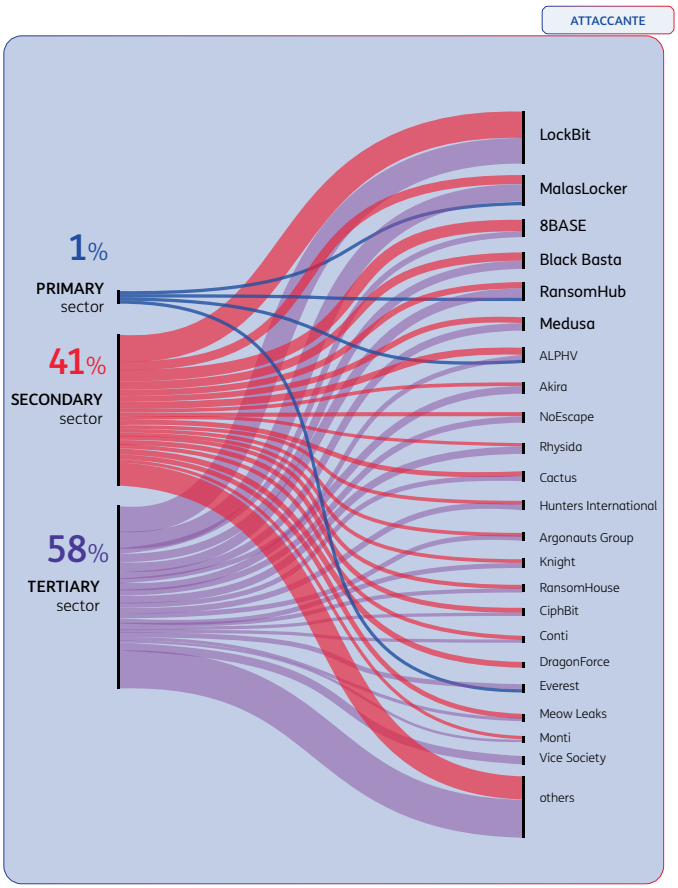
Most of the events detected in 2024 targeted "Home Users" (households and individuals), representing a much wider target to reach, while just under a quarter were directed at public or private organisations. The public administration was the sector with the highest growth in DDoS

events between 2023 and 2024, rising from 1% to 42% of the total cases targeting the sectors. Conversely, the number of events targeting professional services decreased (from 36% to 17%), but is still the primary target among businesses. Other sectors with a growing share compared to 2023 were: Finance (from 3% to 14%), Defence (from 4% to 6%) and Media (from 1% to 2%).

DDoS attacks targeting businesses may have different motivations: opportunistic reasons, acts of digital vandalism, unfair competition, political activism movements, or demonstrations of power by hacker groups. Yet, the high volume of events affecting the institutional sector in 2024 suggests a potential correlation with the geopolitical context.

2.2. Ransomware and Malware

Analysing the ransomware phenomenon is not easy, due to the difficulty in collecting data and in reporting the attacks. This leads to discrepancies in the collected data, making it difficult to gain a complete understanding of the phenomenon. In 2024, the most affected Country globally was the USA: of over 5,200 cases, about one in two attacks targeted US companies. Italy, with 146 cases, ranks fifth in the world and second in the EU, behind Germany. Among the non-EU countries, the most affected was the UK, with 262 cases.



Between 2022 and 2024, the majority of ransomware attacks reported targeted the services sector (58% of total events), but overall, manufacturing was the most affected sector, with 26% of the attacks.

Focusing on 2024, 42 ransomware groups were identified as threatening Italy The most active were RansomHub, Lockbit, 8BASE and Black Basta.

A malware distribution campaign is a concerted action that aims to propagate malicious software, known as malware (MALicious softWARE), through different channels to compromise IT systems, networks and devices, with the use of different tools (viruses, worms, trojans, spyware etc.), each with specific operating modes.

In 2024, 168 malware campaigns were recorded in Italy aimed to compromise IT systems through different means, exploiting system vulnerabilities or social engineering techniques, which aim to lure users in order to steal their passwords or confidential information. The major threats came from Remote Access Trojans, installing themselves on a computer, a mobile device or an appliance and opening a loophole that allows attackers to control the infected machine remotely.

3) Cybersecurity and regulation in the EU: an evolving framework

In this context of significant threats affecting companies and supply chains across national borders, common defence systems should be established, starting from the exchange of information and the definition of common practices. This is why the European Union has long since launched a process to establish a common cyber defence system, which, in the current geopolitical context, represents an enabling condition for technological sovereignty and the competitiveness of the digital economy. This is a complex challenge, which must deal with continuous technical innovation (5G, cloud computing, artificial intelligence), variable geopolitical factors (Brexit in the recent past, changes in political and trade relations today), unforeseen emergencies (pandemic), new consumption and working methods, changes in the social awareness towards specific issues (data protection). All these factors continually change the framework and define new spaces where cyber threats can infiltrate.

The EU addresses this complexity by constantly adapting its cybersecurity policy and the rules monitoring the protection of the digital space.

In 2024, NIS2 came into force, extending the number of sectors and companies that must implement specific security measures under the obligation to report cyber incidents. Apart from NIS2, in 2024 further regulatory instruments were introduced:

- Cybersecurity Act (CSA), defining a common framework for the EU, strengthening the role of the European Cybersecurity Agency ENISA by defining common rules among Member States.

- Cyber Resilience Act (CRA), defining cybersecurity requirements for products with digital components (i.e., medical instruments and smart toys).

In addition to the above, there are:

- CER Directive: for the protection of critical infrastructure.
- EUid Regulation: for a sovereign and secure management of digital identities.
- DORA: for the digital operational resilience of financial sector players.

Today, the establishment of the European cyberspace as a safe and regulated environment is a cornerstone of the EU industrial policy. However, complexity and regulatory stratification pose challenges of harmonisation, efficient implementation and inclusion of SMEs, which need tools and support not to be excluded from the innovation. In this context, through the ACN and the most structured private operators, Italy can play a leading role in transforming compliance into a lever for digital competitiveness and trust.

4) New technical fronts under scrutiny: threats and opportunities

4.1. AI and Cybersecurity

Artificial Intelligence (AI) is becoming a key factor in cybersecurity, acting simultaneously as advanced defensive tool and as offensive lever in the hands of attackers. AI-based cyber security technologies and solutions can: support and enhance prevention and threat detection due to predictive and adapting capabilities; improve the understanding of customer and system behaviour, allowing the distinction between legitimate activities and anomalous ones; accelerate incident response processes, data analysis, network protection and vulnerability identification. At the same time, AI also facilitates the evolution of cybercriminal techniques. Generative AI is used for malicious purposes (writing of malware, advanced phishing, exploit development, advanced reconnaissance using deepfakes) in alternative tools such as WormGPT and FraudGPT.

Hence, AI can amplify the destructive potential of cyber-attacks, by lowering the technical barriers to entry and making the malicious campaigns more sophisticated, realistic and difficult to detect. Organisations and institutions are called to face the antagonistic and malicious use of AI with an equal technological development of defensive tools and processes, always in compliance with the relevant regulations (GDPR and AI Act).

4.2. Quantum Technology

Quantum technologies are emerging as the new frontier in digital transformation, with potential applications both in defensive and offensive cybersecurity solutions, due to their extraordinary computational capabilities and ability to manage complex systems. As with AI technologies, quantum computing has both potential threats profiles, and opportunities to improve defence parameters.

Among potential threats, we find the capabilities of quantum computing in making current cryptographic algorithms vulnerable in a short time. To mitigate this risk, both the US and the EU have implemented strategic programmes to adopt quantum cryptography, aiming to make cryptography infrastructures resilient in light of the expected increase in quantum computing penetration in the coming years.

In fact, quantum technologies open new opportunities to enhance security and defences in the cryptography and microprocessors sectors, enabling cybersecurity applications based on quantum technologies. In this perspective, Telsy developed a Secure Microchip, a programmable and secure-by-design micro-platform based on PQC algorithms, to ensure defence even against quantum opponents. GSMA selected it as one of the best technological innovations.

Quantum computing hence represents a technological discontinuity designed to redefine cybersecurity paradigms. While it poses serious threats to the current cryptographic infrastructures, it also offers new tools to strengthen the security of the most sensitive information, making the initiation of transition strategies towards quantum-resilient models a priority.

INDEX

A new cybersecurity report

TIM is one of the main European telecommunications operators and this position gives us a unique perspective on the cybersecurity threats' scenario. Throughout the last year, our Cyber-SOCs have analysed multiple security events daily to prevent potential incidents or mitigate their effects. An unceasing daily activity which engages us day and night to protect our network infrastructure, cloud platforms, service systems, and customers.

TIM Group includes several entities that coordinate with each other to address cybersecurity threats: network security, SOC, Telsy's and TS-Way's activities. **From our privileged vantage-point we can offer a unique and unparalleled view of the scale of cyber-attacks in Italy**, observe and analyse the features of the attacks launched, highlight the dynamics and aspects specifically related to the Italian context, monitor threat trends and the activity of criminal groups

Attacks target citizens and businesses, households, bodies and institutions. All sectors without distinction are under cyber-attacks. Some are more sensitive targets due to intrinsic and structural reasons, others for opportunistic reasons, for example a defence level being perceived as weaker by the attackers. **This motivated us to dedicate part of our analysis to sector observation**, to identify potentially critical areas and to promote a higher awareness of the system.

Our vision is that the stronger the system, the more effective the defence we can deploy. This concept is also the foundation of the European cyber-security system. **That is why we aim to provide a summary of how the regulatory and institutional context is evolving**, highlighting the measures being taken to enhance defences and what is being done at European level to counter the ever-increasing attacks.

We firmly believe in the potential of the digital world. It is our market and our mission. However, the **technological development must ensure both innovation and security**. Only a reliable system can give us the opportunity to fully experience the present and the digital future, through services that simplify and enrich our daily life.

This vision also entails the need to raise everyone's awareness about protection from cyber threats and **this report contributes to spreading a "cybersecurity culture"**, addressing not only sector professionals, but especially non-experts, people who want to gain a clearer understanding of the trend of the cyber-security landscape. For this reason, we have included charts and infographics, to simplify a very complex topic that concerns us all closely.

Our **vision** is that the stronger the system, **the more effective defence** we can deploy and for this reason **we need to raise everyone's awareness**

How to read the report

Structured in 4 parts

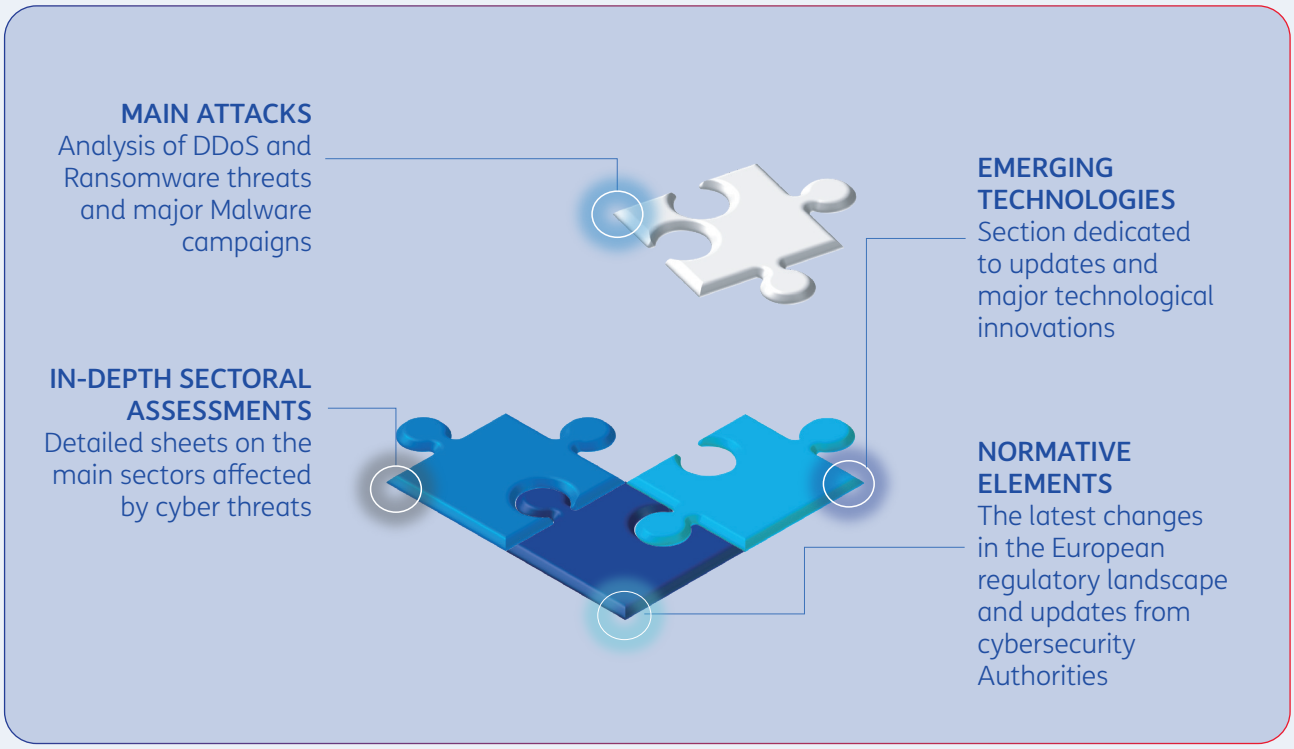
The report is based on four axes of in-depth analysis and constant monitoring:

ATTACKS: in this section, the main findings collected over the year are analysed, based largely on data from the activities carried out, particularly related to DDoS (Distributed Denial of Service), Ransomware and Malware events.

AREAS: many of the cyber-attacks detected are targeted at the consumer world, i.e. households and individuals. However, the most disruptive attacks are aimed at businesses and the industrial sectors, or at institutions representing the heart of our observation. In this section we present a «reading» of the data collected per attack area, identifying the sectors and the institutional actors which are most affected and trying to illustrate attack directions.

ASSETS: our national cyber-defence system is based on strategies and regulations defined at European level. This section provides an overview of what is happening in the EU.

UPDATES: the cybersecurity landscape is constantly evolving, influenced primarily by technological innovations that can quickly change the rules of the sector. This section delves into the latest developments in the field, both in terms of defence and of attacks strategies.



An authoritative point of view on the cyber threats landscape

Gianluca Galasso, Director of Operations at the National Cybersecurity Agency, introduces us to the risks of today and tomorrow and provides an update on the expected developments in the regulatory framework.

01 TODAY'S CYBER RISKS: AN OVERVIEW

As to the Report on DDoS and Ransomware attacks produced by the Cyber Security Foundation in cooperation with TIM, **what considerations arise on the current cybersecurity landscape in Italy**, emerging trends and critical vulnerabilities included? Besides, what specific contribution do you see in the **partnership between private entities and the National Cybersecurity Agency (NCA) in preventing and contrasting** these threats and in improving the resilience of the country's infrastructure?

Our Country is increasingly targeted by various types of cyber-attacks. The figures from the National Cybersecurity Agency operational activities are constantly rising, consistently placing Italy among the most targeted countries at European and global level, alongside the most prosperous countries. Thus, we can safely state that the strongest economies, characterised by a high level of digitalisation, primarily attract cyber-criminals driven by profit. Besides, the current complex geopolitical situation is contributing to an increase in cyber phenomena with purposes beyond direct economic gain. **Ransomware and DDoS attacks**, in particular, keep the Agency's incident response teams constantly occupied. The former, increasingly sophisticated, mostly threat private operators, especially those working in manufacturing, while DDoS attacks, even if less disruptive than the former and linked to the current geopolitical context, have recently taken on a more aggressive profile. Furthermore, **spear-phishing campaigns** are becoming increasingly sophisticated, often enabled by AI applications to develop complex attack strategies targeting people before systems, exploiting their weaknesses such as inadequate passwords, incorrect behaviour in the use of devices, carelessness.

This situation is expected to persist over time. Therefore, the objective for the entire national cyber ecosystem should be to make digital infrastructures increasingly resilient to different forms of threat by adopting organisational and technological solutions that minimise the impacts of cyber-attacks. This is why the Agency has promptly committed to developing the technical-operational capabilities necessary to detect and anticipate the cyber threats affecting the country, with a focus on critical infrastructures, benefiting both public and private operators and developing a full capacity of intervention in the event of an incident, especially in support of the most critical service providers.

In this context, **the private sector role**, above all that of the most structured operators which provide essential services is extremely important, as cybersecurity is enabled by the exchange of knowledge at all levels. For this reason, during the first two years of the Agency's activity, some important initiatives have been launched with the direct involvement of private operators, which are both originators of technical and operational information towards the Agency and users of information supplemented by the Agency itself. We refer in particular to the HyperSoc capacity, a platform to exchange data related to malicious events being developed with the support of private operators, already operational today in a baseline version and joined by some important national entities. This tool, that in 2025 saw new technical implementations and is opening to an ever-increasing number of participants, represents a significant example of public-private cooperation on which the Agency has high expectations.

02 ARTIFICIAL INTELLIGENCE AND CYBERSECURITY

Artificial Intelligence (AI) is transforming many sectors, cybersecurity included. How can advanced AI technologies and capabilities, applied to security measures, support organisations in implementing pro-active and reactive security measures, such as anomaly detection, automated incident response and threat prediction? Also, what do you consider to be the **main risks** that organisations will have to face with the evolution of AI-based attack techniques, through advanced machine learning algorithms detecting and exploiting vulnerabilities, and which areas should be most closely monitored to mitigate these risks?

The use of AI to strengthen one's security posture is not entirely new; the various solutions already present on the market for several years leverage different applications of artificial intelligence to analyse malware or detect anomalies in network traffic. However, recent technological innovations in this field are greatly expanding the potential applications of AI.

In particular, together with the AI models typically used to support the work of first-level analysts, generative models can also be used, to assist in solving multiple tasks through a simple text interface, effectively making this technology much more accessible. This undoubtedly will have a significant impact on the operational management of proactive and reactive cybersecurity activities. In fact, thanks to new AI applications, it is also possible to provide an analyst with details regarding alarms, suggestions on the actions to be taken for incident response, a textual description of code functionality or an automated system for the production and analysis of reports. Thus, the use of new technologies will allow for the improvement and automation of analysts' activities, especially when faced with large quantities of data to be analysed and correlations to be performed, to the benefit of the cyber posture of the IT infrastructures to be protected.

In this scenario, moreover, it is important to take care of the training of analysts in order to avoid, over time, the loss of the technical skills necessary to understand and, if necessary, validate the results provided by the machines.

AI is also a powerful tool that can increase the capabilities of attackers. This is already a reality, as demonstrated by the evidence emerging in some operational contexts and by the fact that the Mitre ATT&CK framework, a globally used taxonomy to describe the tactics and techniques of cyber-attacks, has recently included the use of AI to achieve offensive capabilities. Several studies highlight how AI can amplify cyber threats, not only in terms of sophistication, but also in the number of threats generated; this means that the new technology will enable more sophisticated and numerous threats than those currently detected.

AI-powered attack tools can be effectively used by attackers with less technical skills than those needed for "conventional" attacks. This means that operators with elementary skills, who would otherwise be incapable of carrying out significant offensive actions, can now execute more complex attacks with a critical impact on their victims.

02 ARTIFICIAL INTELLIGENCE AND CYBERSECURITY

Consider the easy access to tools for creating fake multimedia content, the so-called “deepfakes”, widely used not only to spread disinformation, but also to carry out sophisticated and extremely dangerous phishing attacks.

To adapt to these changes in the sophistication and magnitude of threats, we have to improve resilience activities by adopting AI-enabled tools to make response and resilience activities more effective. The adoption of new technologies, such as the so-called GenAI SOC, will help address the growing complexity of Security Operation Centres, the chronic shortage of specialised technical personnel, the ever-increasing volumes of systems “alerts” and the complexity of analyses that require more and more time and skills.

03 DEVELOPMENTS OF THE REGULATORY FRAMEWORK

The new EC and national regulatory framework on cybersecurity, with the NIS2 Directive, the DORA Regulation, the AI and PSNC Acts etc., presents new challenges and opportunities for Italian organisations. **How can these procedures support organisations in improving the maturity of their cybersecurity posture and measures?**

The new EC and national regulatory framework on cybersecurity aims to strengthen resilience and cybersecurity at both national and European levels, establishing higher standards and an integrated approach to managing cyber risks.

The shared goal is to respond to the rapid evolution of the technological landscape and the increasing complexity of cyber threats, with the common denominator being risk analysis and management (risk assessment, planning and implementation of appropriate security measures, continuous monitoring, and incident response).

Understanding and managing these aspects is a responsibility that no entity can afford to ignore, as it ensures a constant improvement of their cybersecurity posture and must be regarded as a strategic priority.

The opportunities to be considered thus lay the foundation for a comprehensive 360-degree management of cyber risk, where governance, policies and procedures support full regulatory compliance and strengthen the whole entity infrastructure. This ensures its increasing capability to protect data and information, guaranteeing operational continuity even in the event of a cyber-attack, and safeguarding its reputation.

Noticeably, these aspects do not depend on the scale of an organisation and equally affect SMEs. These companies, which often have limited resources compared to larger ones, face significant challenges in complying with complex regulations. However, to ensure that SMEs also may benefit from this regulatory framework, targeted support from the national system is essential, including training, financial incentives and accessible compliance tools.

04 CHALLENGES FOR THE COMING YEARS

In light of the «2022–2026 National Cybersecurity Strategy», **what are the main areas and challenges that a NCA will have to face in the coming years?** How does the NCA consider the way private organisations, the ones providing essential services included, may cooperate effectively to ensure the security of the Country? In particular, what are the cooperation strategies the NCA believes may be adopted to mitigate cyber threats and protect critical infrastructure from attacks and security breaches?

Rapid technological evolution, intricately linked to digitalisation, brings constant new security risks alongside its innovative features. Society often lacks adequate awareness to respond to these risks. With the **2022-2026 National Cybersecurity Strategy**, the NCA has therefore set up a plan to design, coordinate and implement a series of measures aimed at making the country safer and more resilient, targeting the following challenges:

- ensuring a **cyber-resilient digital transition** for the Public Administration (PA) and the productive sectors;
- anticipating the **evolution of cyber threats**;
- preventing and managing **cyber crises;**
- ensuring national and European **strategic autonomy** in the digital sector.

To best address these aspects, **three main objectives** have been identified, grouping measures by thematic areas to ensure the effective implementation of the Strategy:

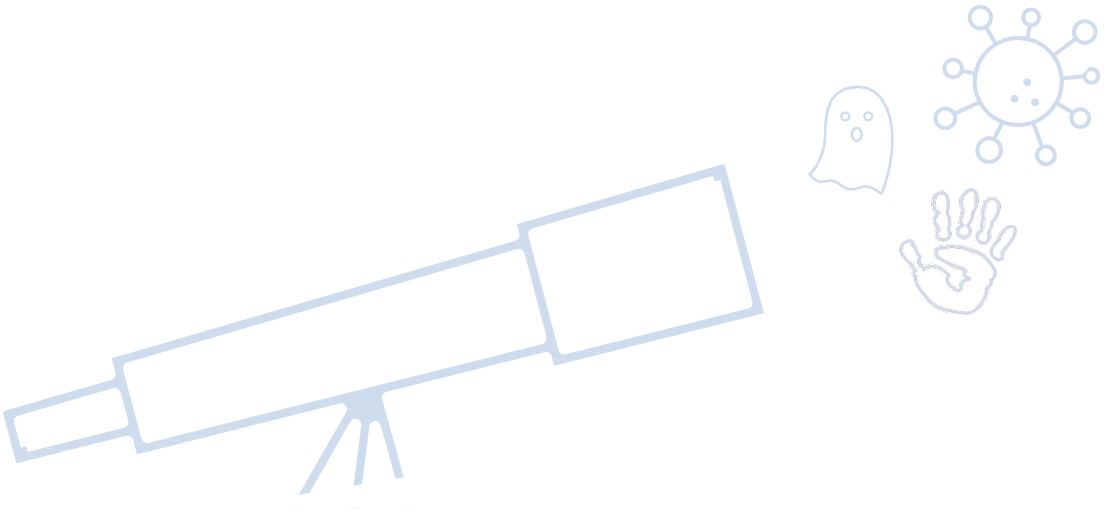
- **•PROTECTION.** Protection of national strategic assets based on a systemic, risk management-oriented approach through the maintenance of a coherent regulatory framework and the application of security measures, tools and controls**.**

- **RESPONSE.** Response to cyber threats, incidents and crises through the deployment of national monitoring, detection, analysis and response capabilities, as well as the activation of alerting procedures involving all actors in the national cybersecurity ecosystem.

- **DEVELOPMENT.** Secure development of digital technologies, support for research and strengthening of industrial competitiveness, in order to respond to market needs through the synergic action of institutions, academia, centres of excellence and businesses.

The digitalisation related to the provision of essential State functions and services has made cybersecurity a fundamental objective for protecting national interests in the cyberspace.

The **National Cybersecurity Agency** has therefore set up a plan to design, coordinate and implement a series of **measures aimed at making the country safer and more resilient**



To ensure the country's security, under "Response" fall the so-called National Cyber Services developed by the Agency to enhance prevention, monitoring, response and mitigation of cyber threats at the national level.

Here is where the HyperSOC, ISAC Italia and the ISAC national network come into play, and where, by strengthening Public-Private Partnerships, organisations may cooperate with the NCA to i) identify early potential complex attack patterns that could represent emerging threats of interest, ii) strengthen the ability to prevent, identify, mitigate and counteract cyber risks through context analyses based on the specificities of each sector.

The chosen approach is that of a **two-way communication among all the actors involved**, so that the exchanged data may turn into validated, analysed and enhanced information to strengthen their level of situational awareness. Thus, protecting critical national infrastructures from cyber threats is not an individual challenge, but rather a collective responsibility where the creation of trusted ecosystems starts precisely from the sharing of information on cyber risks. Cybersecurity is a risk issue and as such it must be addressed together.

To ensure Country security, under "Response" fall the so-called National Cyber Services developed by the Agency to enhance prevention, monitoring, response and mitigation of cyber threats at national level.

Main attacks

As digitalisation extends to more activities, affecting all areas of our lives, the areas exposed to cyber threats are increasing, and this concerns everyone: institutions, businesses, bodies, ordinary citizens. The only certainty is that we are all potentially subject to the effects of a cyber-attack: blocking of activities, inability to gain access to computers, servers, sites or other IT resources, removal of data and information, whether sensitive or not. Building a 100% secure system is impossible, but building a resilient system is achievable, starting with a better understanding of how these events occur. In this first part we focus on the events that our cyber defence groups have detected over the last year. We talk about events because the threats we face do not always translate into attacks and incidents.
Prevention, defence and mitigation activities performed by our teams, especially those acting within the Security Operation Center (SOC) and those engaged in Threat Intelligence preventive activities, are essential.

The attacks

How to classify them

The main problems encountered when entering the cybersecurity world concern primarily the understanding of what we are observing. The complexity of the topic is even more accentuated by the number of views we can assume, which lead us towards different taxonomies and multiple classifications of case studies.

Each one has its purpose.

For example, one of the most frequent is the MITRE ATT&CK taxonomy, with the objective to build a common knowledge base. This is why it divides the field of observation into three «domains» –Enterprise (referred to business networks and cloud systems); Mobile; Industrial Control Systems – and for each one it identifies the tactics (defined as the motives), the means (i.e. the techniques applied), the variants (sub-techniques), and the procedures which could be implemented by some opponents. The map is constantly evolving. For example, for the Enterprise segment only, between April 2024 and February 2025 the tactics did not vary (14), the techniques increased by one (from 202 to 203) while the variants rose (from 435 to 453).

Another reference is the VERIS taxonomy (Vocabulary for Event Recording and Incident Sharing), developed by a group of experts appointed by the European Commission to create a common language to describe the security incidents in a structured and reproduceable way. This taxonomy observes each recorded event under 4 perspectives: who is behind an incident (Actors), which means are used (Actions), which devices are attacked (Assets) and how they are affected (Attributes). In turn, each of these areas is declined in several potential options to define a common framework to describe the recorded events.

For **our purposes**, which seek to provide a view of cyber-attacks by favouring an **easier understanding of the phenomenon, we shall present the data collected under the ENISA classification**.

The above taxonomies have enormous value for industry experts but are too complex for those with less expertise. This is why we follow the approach by ENISA, the European Cybersecurity Agency, which in its annual reports identifies 8 main categories of threats that are more immediate and understandable.

The main cyber threats

Within the European Threat Landscape, ENISA, the European Cybersecurity Agency, identifies 8 types of cyber-attacks, i.e. deliberate events designed to penetrate the defence mechanisms of organisations, companies and individuals for different purposes.

DOS and DDoS attacks
(Distributed Denial Of Service)

Attacks aimed at making a resource/ service unusable by overloading the network infrastructure components

Data threats

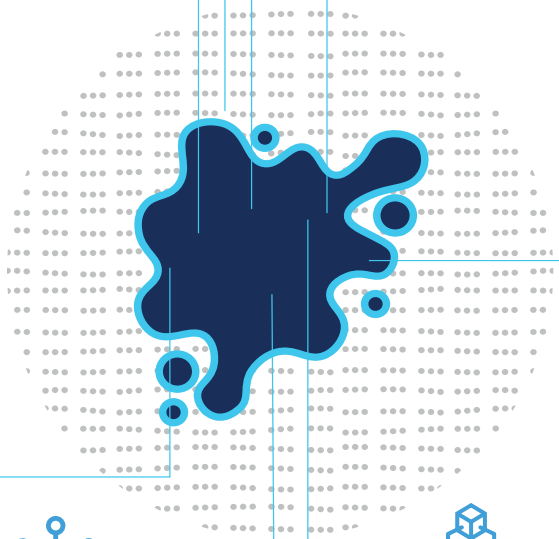
Unauthorised access to data by subtraction, disclosure and manipulation. Often combined with ransomware and DDoS attacks

Ransomware

The attack aims to penetrate the systems (networks, computers, clouds, etc.), take control of the resources (data, assets, etc.) and ask for a ransom

Malware

Software or firmware that runs an unauthorised process with a negative impact on the integrity or the availability or the functioning of a system



Social engineering threats

They include a wide range of activities which profit from errors to get access to information or services.

Threats to networks and the Internet

Incidents where there is an intentional or non-intentional disruption of the access to the Internet or to electronic communications.

Attacks to supply chains

Attacks targeting the relationship between the organisations and their providers (e.g. penetrating a company network to exfiltrate data from the client company)

Disinformation

Companies and individuals targeted by disinformation campaigns aimed mainly at discrediting their reputation or create uncertainty

DDOS attacks

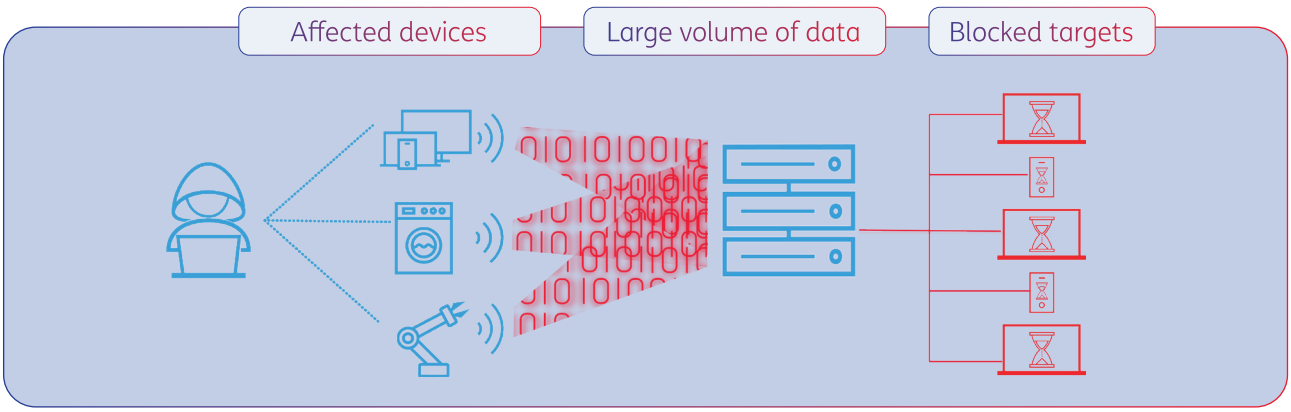
A DOS or «Denial of Service» attack falls among the threats to an asset/service availability. In this report we focus on volumetric attacks where an attacker can direct a significant traffic volume towards a network resource, a website or a server overloading it and preventing it from providing the service. This can be done also by activating unsuspecting people's devices and equipment which the attacker takes control of. Hence, the attack comes from multiple directions, and it is known as «distributed».

A customer wanting to use a system or access data or other relevant resources under DDoS attack cannot do so, as the huge data flow (or, in case of non-volumetric DDoS attacks, the number of requests) paralyses its functionalities. The effect is similar to trying to acquire a ticket for a highly requested event and the system not responding. This occurs because the traffic aimed at the target overwhelms the ability of the attacked resource (a server, a site, etc.) to manage the sudden flow.

Although it is clear how the aggression takes place, the ENISA points out that it is not always easy to identify it for the following reasons:

- The attacks may start slowly or proceed in waves without a clear start/finish, making it difficult to identify different events.
- An attack may tackle several sites from the same IP address, making it difficult to assess both target and attack duration.
- The attacks may originate from several geographic areas.
- Monitoring systems can also be targeted, making the detection more difficult.

Furthermore, specific cases are constantly emerging: with the artificial intelligence (AI) the attackers may orchestrate and mask the assaults. The SOCs of the TIM Group work across the network, therefore they can detect the attacks and intervene before they manifest themselves. The data of this monitoring, prevention and mitigation activity is provided below.



DDOS attacks
Recap **2024**

DDoS attacks return to pandemic levels

+36%

2024 vs 2023 DDoS events

In 2024 we recorded a strong surge of DDoS attacks per volume, intensity, duration and severity. This is due to the ongoing conflicts, as well as to new attack techniques.

>20Gbps

4 out of 10 events have a power higher than 20 Gbps

The sectors most affected by DDoS events

Institutions
Professional services
Finance
Telecommunications
Defence

More than 25%

of the events are severe with maximum power and more-than-two-hours duration

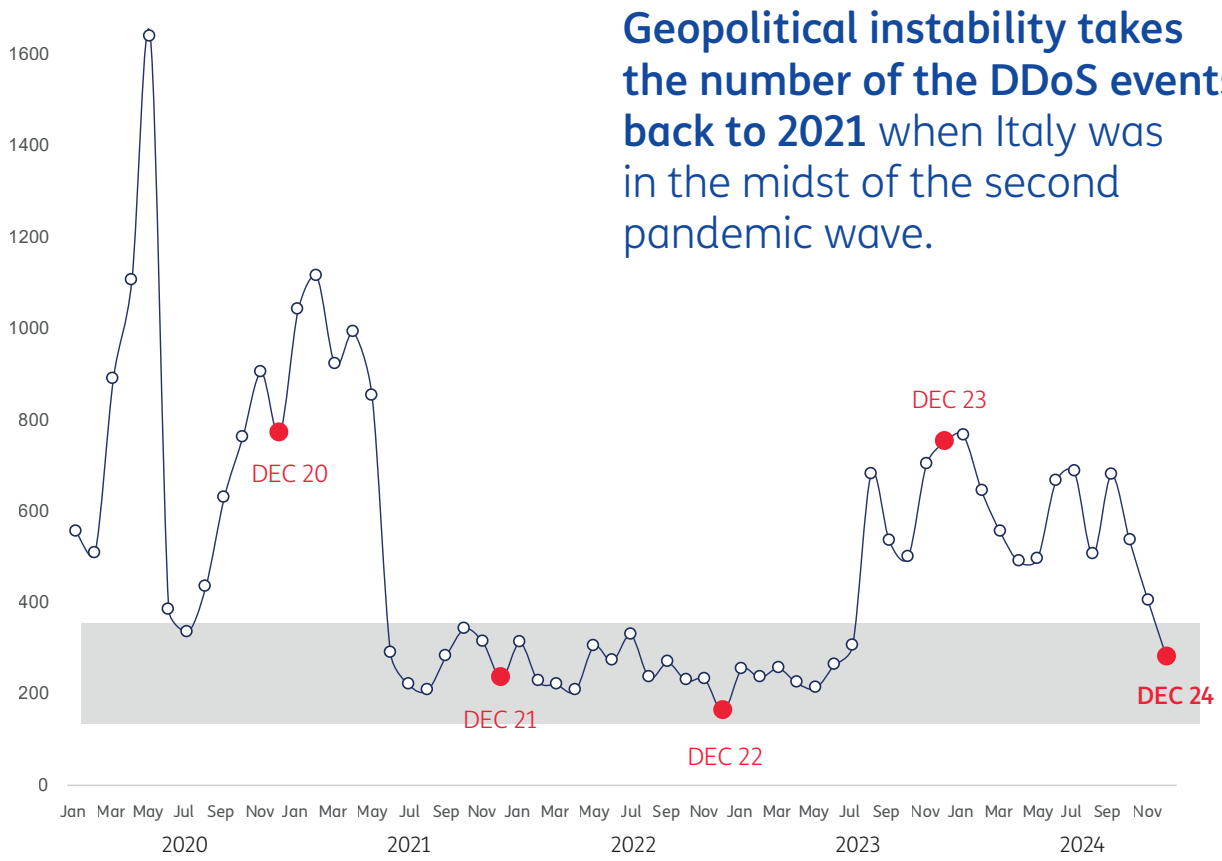
x4 increase in severity compared to 2020 (severe events were 6% of the total)

DDOS attacks
2024: an **intense** year

2024 registered a strong surge in terms of DDoS events: on average, around 560 cases per month with two peak moments and a gradual decrease in the last quarter of the year. Looking at the dynamic of the events in a broader timeframe (2020-2024), three distinct periods of similar length can be identified:

- **January 2020 - August 2021**, with an average of around 725 events per month and two peaks of 1,600 and 1,100 cases. The high -intensity of this period, with the Country facing lockdowns, is due to the broadening of the attack scope (remote working, online teaching, etc.).
- **September 2021 - July 2023**, of low-intensity, with an average of approximately 260 events per month.
- **August 2023 - December 2024**, with an average of 580 cases per month, with a peak of 765 events that is at levels similar to those of the pandemic period due to the unpredictability of the geopolitical framework.

DDoS events in Italy detected by TIM SOC in 2020-2024



Geopolitical instability takes the number of the DDoS events back to 2021 when Italy was in the midst of the second pandemic wave.

The boom of DDoS attacks

1) The influence of **conflicts**

The spread of new DDoS attacks techniques increases the power of this kind of events, as can be seen later in the report. However, along with these "internal" causes there are other motives related to context, such as the lockdowns in 2020-2021 and the recent geopolitical tensions.

In fact, a DDoS attack has multiple motives (economic, ideological, personal) and can be used also as a cyber-warfare tool in the so-called hybrid war to cause economic damage, disrupt potential rivals' infrastructures and essential services, or give a demonstration of force.

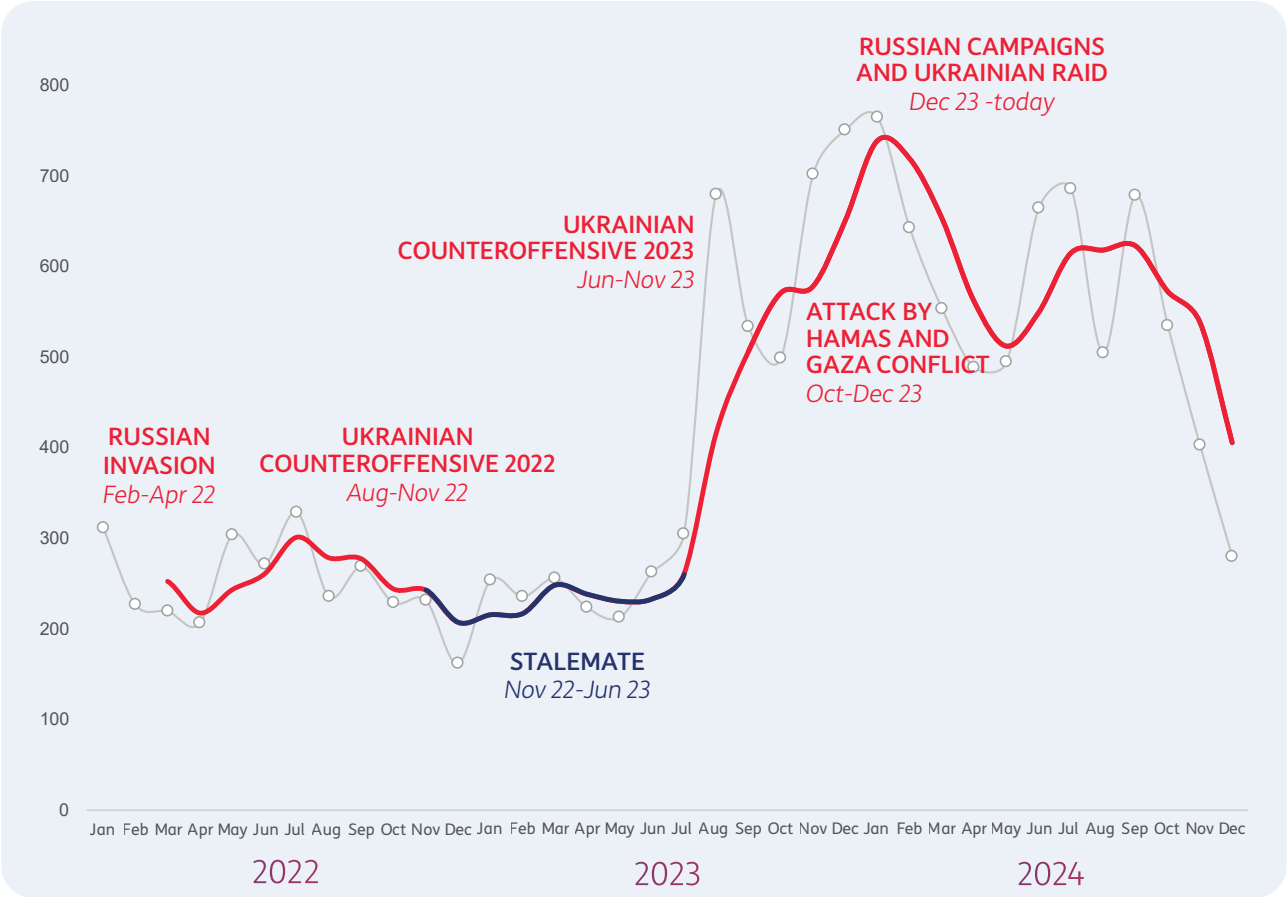
The growth of DDoS events in recent months is surely related to the ongoing conflicts and has affected the European countries for the support expressed towards the belligerents. In 2022 and in the first half of 2023, the DDoS events showed a moderate trend, but began to surge starting in August, where a first surge is recorded. Between November 2023 and January 2024, at a time when the Russian-Ukrainian conflict is intensifying and the one between Israel and Hamas is breaking out, a second surge is registered. From this point of view, the DDoS events phenomenon can resemble a thermometer measuring geopolitical stability. ENISA too highlights an increase in DDoS incidents which in the period July 2023-June 2024 doubled in terms of incidence compared to all registered events: from 21 to 41% of the total.

DDoS attacks on the rise also due to ongoing conflicts

DDoS ATTACKS, A CYBERWARFARE WEAPON

The motives behind the DDoS attacks have a financial and a geopolitical nature. The Ukrainian conflict saw the resurgence of politically motivated activists and there was a further worsening due to the conflict in the Gaza strip.

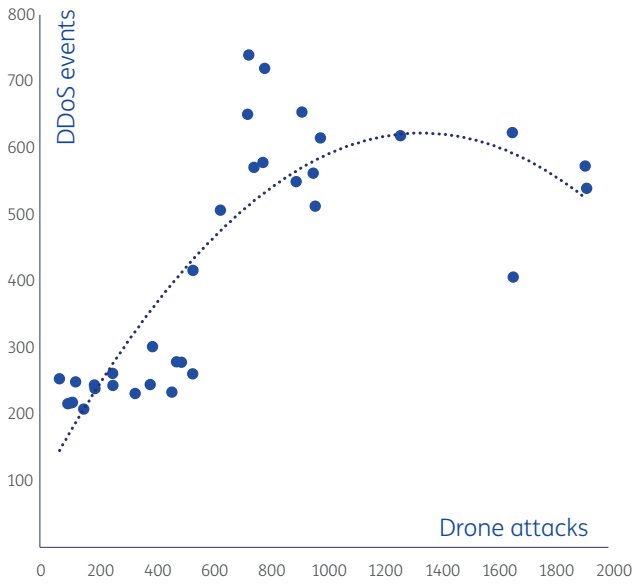
DDoS ATTACKS IN ITALY DETECTED BY TIM SOC
as to the phases of ongoing conflicts – years 2023-2024



Russian-Ukrainian Conflict Phases https://en.wikipedia.org/wiki/Timeline_of_the_Russian_invasion_of_Ukraine#

We tried to correlate the evolution of the DDoS events from 2022 to 2024 with the data collected by ACLED (an independent non-profit NGO) on the Russia-Ukraine conflict, in particular regarding drone attacks, which represent a technological escalation starting from mid-2023.

Albeit with due distinctions, an empirical correlation between the two series can be observed. This also can support the thesis of a geopolitical origin behind the surge in attacks registered between mid-2023 and 2024.



Data source: ACLED.
The data related to the attacks by drones was extracted from "ACLED Armed Conflict Location and Event Data". The source is the database "Ukraine and Black Sea", at the following link https://acleddata.com/ukraine-conflict-monitor/#data (data updated on 28th February 2025, mobile average 3 months)

The boom of DDoS attacks

2) New technologies and **attack techniques**

During 2023 and 2024, threats based on other techniques also increased. An example are the hyper-volumetric DDoS attacks directing tens or hundreds of millions requests per second to specific applications preventing their functionality. From this point of view, the attackers can exploit the broadening of potential attack vectors, i.e. affected equipment they take control of, thus fuelling the requests or the traffic. We detected attacks launched by IoT systems as well as by Virtual Private Servers (VPS) or – more generally – by Virtual Machines (VM), which generate 5,000 times more traffic due to their computational resources and available bandwidth.

The combined use of multiple attack vectors puts the legacy defence mechanisms more at risk and enables attackers to target different network levels and elements within the organisational infrastructure, acting simultaneously on websites, network/infrastructure, or devices to inflict the maximum damage possible.

Another trend is due to UDP attacks targeting network protocols allowing the exchange of TCP packets and the interaction between systems. This is also the case in which large number of requests prevents the UDP protocol from working effectively. Lastly, there have been various attacks at application-level targeting websites and API access points, protocols which allow the automatic interaction of the applications with each other. Since this is cryptographed traffic, detecting malicious activities which imitate legitimate requests becomes complex. In addition, there is the use of evasion techniques such as dynamic IP addresses, random http headers, and others. Finally, there are the attacks at the DNS level, the system which «translates» IP addresses from numbers (ex. 192.158.X.YY) to intelligible addresses (www.nomedifantasia.com). The DNS server is flooded with several forwarding requests that it cannot verify, and crashes.

Hyper-volumetric attacks

Attacks that enable attackers to increase the power of the attack (in the order of Terabit/sec sometimes using multiple vectors).

VM/VPS botnet attacks

Attacks launched by virtual machines (VM) or virtual private servers (VPS) generating traffic up to 5,000 times higher than that of a single device.

Multi-vector attacks

Combination of multiple attack vectors within a single campaign to make the legacy defence mechanisms more vulnerable.

Attacks at application level

They target an increasing number of websites and management interfaces (API gateways), imitating legitimate requests and making detection difficult.

Volume of DDoS events

Nearly 5 events of the **highest intensity** per day

A RELEVANT PARAMETER: THE INTENSITY CLASS OF THE ATTACK

Even though the average number of DDoS events registered in 2024 stands at levels comparable to the second pandemic period, the features of the attacks are very different.

Intensity is one of the parameters detected: the higher it is, the stronger the aggressive capacity employed by the attackers. This does not mean that the weakest attacks are less dangerous, since they are able to blend in with legitimate traffic, becoming more difficult to detect and thus succeeding in a more insidious way. In our analysis we divide the events into 6 intensity classes: the first three groups reach up to 10 Gigabit per second (Gbps) while the last two include cases from 20 Gbps onwards. The variation in intensity over time shows, with evidence, how new attack techniques are changing the landscape of DDoS attacks.

AROUND 6,700 EVENTS DURING 2024, MAINLY AT LOW INTENSITY

In 2024, almost 47% of the 6,700 detected events had an intensity lower than 10 Gbps. Although nearly half of the events were of low intensity, their weight on the total number of detected cases is gradually decreasing.

Up to 2021, low-intensity events represented at least 80% of the total, while those with flows higher than 20 Gbps were around 5%. In 2023, low-intensity events had already dropped to 56% of the total and those with a capacity higher than 20 Gbps had reached 30%. In 2024, the weight of cases with an intensity higher than 20 Gbps reached nearly 39%. In particular, the last class, with events of an intensity higher than 40 Gbps, has become the one with the most significant weight (26%).

STILL, VERY HIGH INTENSITY ATTACKS ARE NEARLY 5 PER DAY, A HIGHLY SIGNIFICANT VALUE

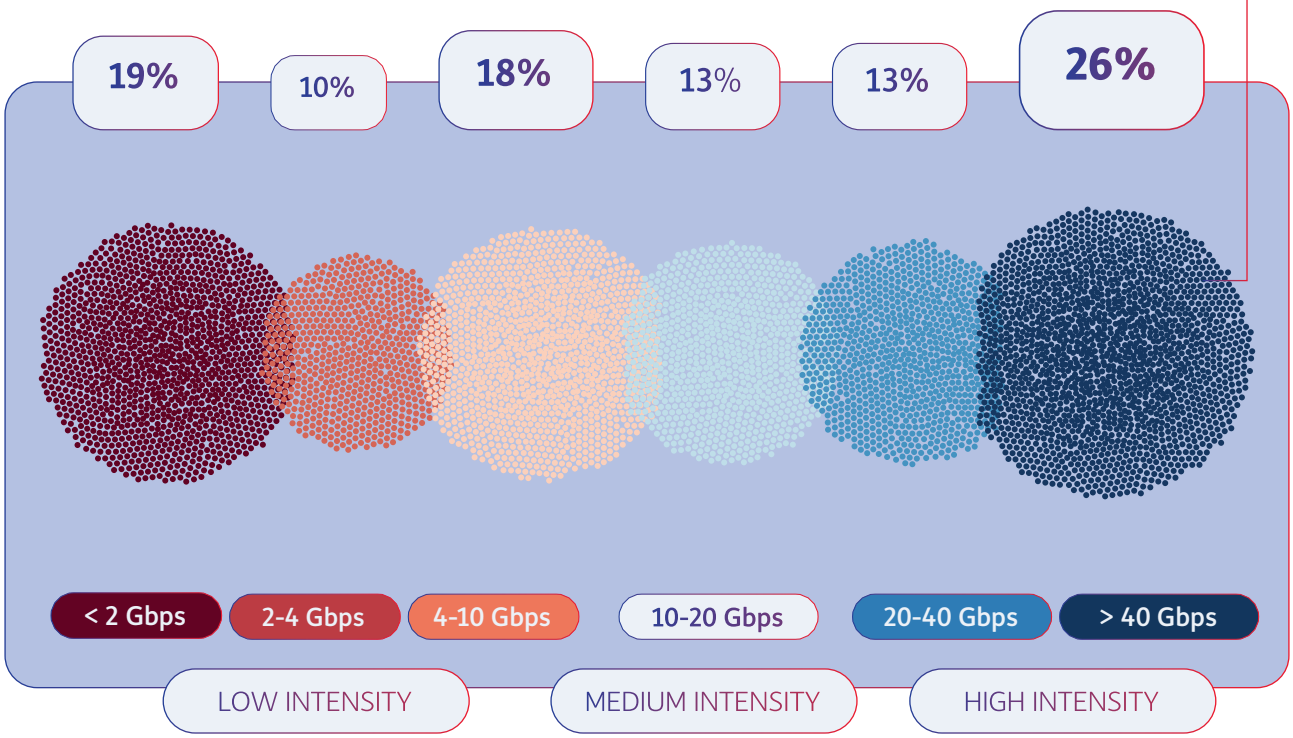
This means that we register an average of 18-19 events per day, of which nearly 7 have an intensity higher than 20 Gbps and 5 exceed 40 Gbps, i.e. around 1 in 4.

Volume of DDoS events
Allocation by **intensity**

This graphic represents the DDoS events detected by TIM Security Operation Center **during 2024.**

They are nearly 6,700 and we have represented them so as to highlight the different intensity levels. **On the left**, in red-orange tones, the less intense events, with a power lower than 10 Gbps. **On the right**, in shades of blue, the more intense events, with power higher than 20 Gbps.

4 in **10** events have **high intensity**

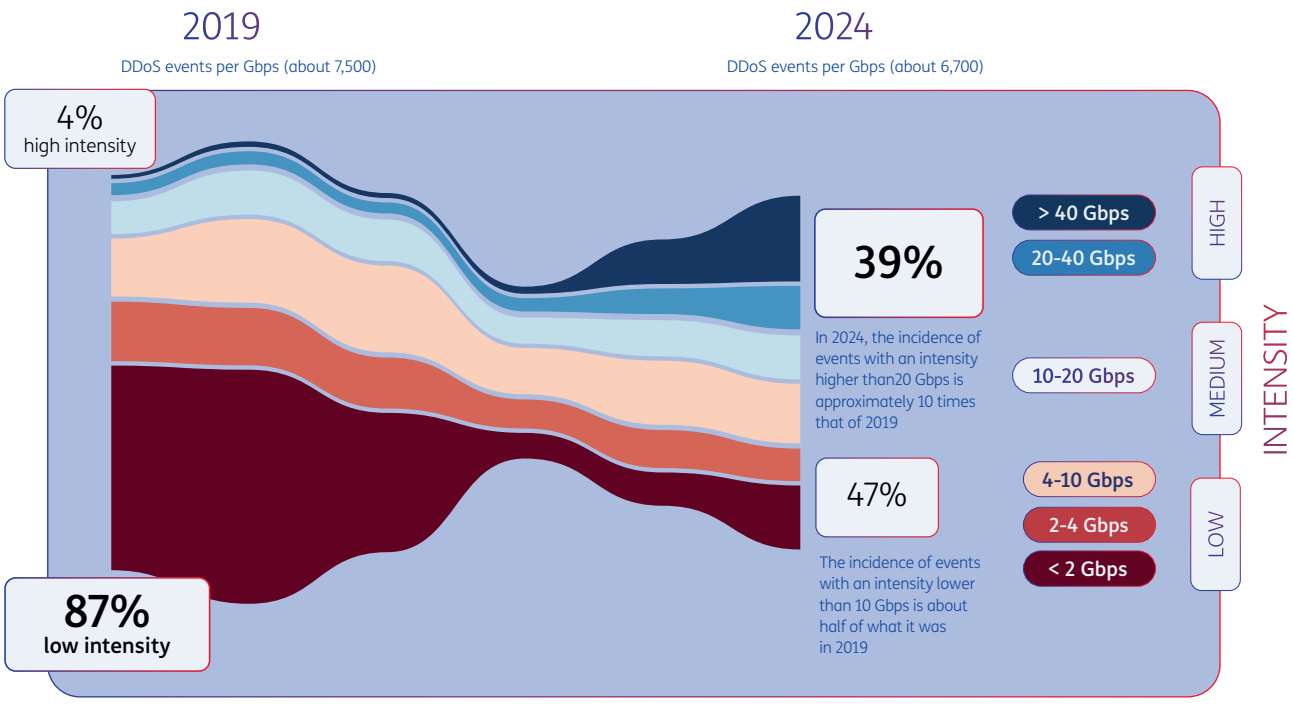


In 2024, compared to 2023, the weight of **high intensity** events doubles

The phenomenon of high-intensity DDoS events can be better observed by comparing the historical series of all cases registered since 2019, categorized per intensity class.

The comparison clearly shows a gradual shift in the distribution proportions: while in 2019 and the following years the weight of the low-intensity events (around 87%) was very high, in recent years the incidence of the high-intensity events – which today represent nearly 40% of the total – has tended to increase. Besides, in 2024 the events have polarised into extreme classes, concentrating those of greater and lesser intensity. This also indicates how the DDoS attacks landscape is changing.

DDoS events in Italy per intensity level: 2019 vs 2024



This intense growth is due to several factors: the decrease in the cost of DDoS payment services per Gigabit/second offered, a higher presence of botnets which can be exploited for illicit purposes, delays in the adoption of anti-spoofing services and the strong escalation of the attacks due to the worsening of the geopolitical context.

Attack peaks: the maximum bandwidth **used**

THE ATTACKS BANDWIDTH

Another feature of the events, connected in turn to the intensity of the attack, is the bandwidth used.

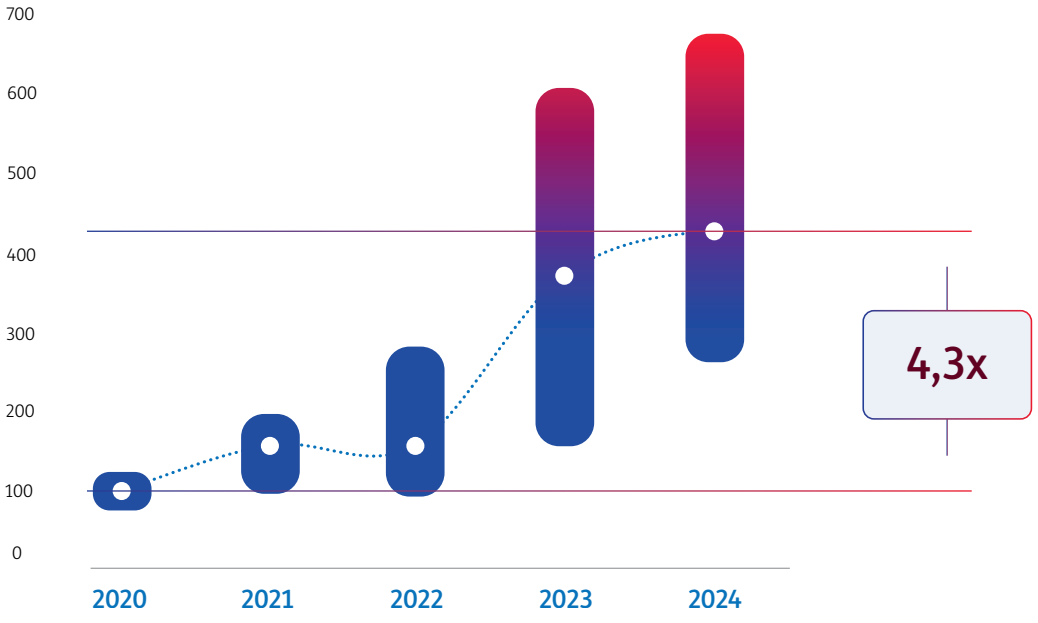
In this case we indicate the maximum peaks reached by a single attack during a given period, typically a month or a quarter.

During 2024, particularly in the first quarter, we also recorded a significant increase in the maximum bandwidth used by a single attack. This element also differentiates the type of attacks registered in 2024 from those in 2020.

Considering the maximum peaks reached by a single event over the course of a month, this value has increased over time. For example, if in 2020 the average of the peaks registered in each month of the year was equal to 100, in 2024 the same value has grown by a factor of by 4.3. The bandwidth of the most significant attack registered in 2024 increased by approx. 6.6 times compared to the absolute maximum of 2020, and the gap between the maximum and minimum peak of the year has widened. Therefore, while the volume of events detected in 2020 remains unmatched, the intensity has increased significantly over time, with strong fluctuations from one month to the next.

DDoS events with Max bandwidth (Gbps)

Index numbers (100= average 2020)



The bandwidth used in DDoS attacks increases.

Between 2020 and 2024, the average of the most significant attacks increases by more than 4 times

Long-lasting attacks: the **hottest** 40 minutes

A SECOND ESSENTIAL PARAMETER: THE DURATION OF THE ATTACK

The intensity level of the attacks should be examined together with the duration of the attack. A DDoS event may have different durations: minutes, hours or even days. In most cases the event has a relatively short duration, but the medium and long duration attacks are growing.

In our classification we specify the very short events (under 10 minutes), short (between 10 and 30 minutes) and the average (from 30 to 120 minutes), long (from 120 minutes to 24 hours) and very long duration (higher than 24 hours) attacks.

9 DDoS ATTACKS OUT OF 10 HAVE A DURATION UNDER 30 MINUTES

Short and very short attacks.
The short and very short events represent 90% of the cases recorded in 2024 and this share is growing: in 2022 they represented around 85%. The short events (between 10 and 30 minutes) account for about half of the registered events.

Attacks lasting over 2 hours.
The categories of the long attacks are still very small and therefore episodic, but they are growing due to higher broadband availability, the use of innovative technologies (AI, Cloud), and new modes of attack. As for attacks lasting over 30 minutes, their number decreases as duration increases. The first group of long attacks, including the cases lasting between 2 and 24 hours, totalled almost 170 (up by 10 units compared to 2023). Conversely, the number of attacks lasting more than a day was halved: from 22 to 11, with values still very low.

Overall, the weight of the attacks lasting more than two hours remains unchanged compared to the total (around 4% of the total).

DDOS EVENTS LASTING MORE THAN TWO HOURS HAVE A WEIGHT IN MINUTES EQUAL TO 57% OF THE TOTAL

The perspective changes if we convert the cases into minutes, taking as reference the median of each timeframe as the duration of each DDoS event*. In this case, around 180 events lasting 2 hours or more have a «weight» of around 57% of the total number of events (in 2023 it was 65%).
* For events lasting more than 24 hours, 1441 minutes, equal to 24 hours + one minute have been considered.

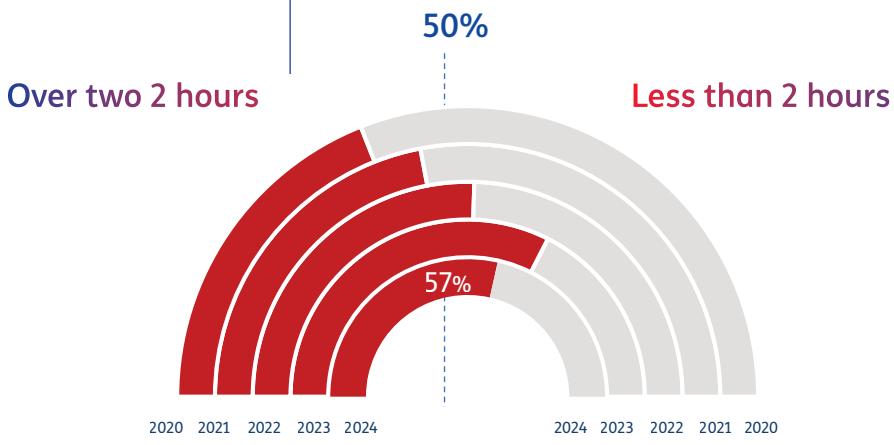
In 2024 the **average duration** of a DDoS event lasted around **39 minutes**.

EVOLUTION OF ATTACK DURATION
over the last five years

Short Attacks

> 10 min	2.866	+59%
10 - 30 min	3.198	+21%
30 - 120 min	454	+52%
120 min - 24 h	169	+6%
> 24 h	11	-50%

Long Attacks



Weight of the attacks in minutes (%)

Analysis carried out on the median duration for each single segment.
For the last class, attacks lasting 1441 minutes, equal to 24 hours + 1 minute, have been considered

The events lasting more than two hours decrease

The overall weight in terms of minutes of attack drops below 60%

Severity of the events: more **power** and **duration**

THE SEVERITY MAP IS A USEFUL TOOL TO OBSERVE THE TRANSFORMATION OF DDoS ATTACKS

DDoS attacks show a significant transformation: the events are still mostly of low intensity and of short and very short duration, but the new techniques are leading to a rise in the intensity and duration of the attacks.

Noticeably, these are the main pieces of evidence we accounted for. The events registered over time present a large variety of techniques and modalities, and the purposes, targets, resources and assets on which the attacks are aimed can change.

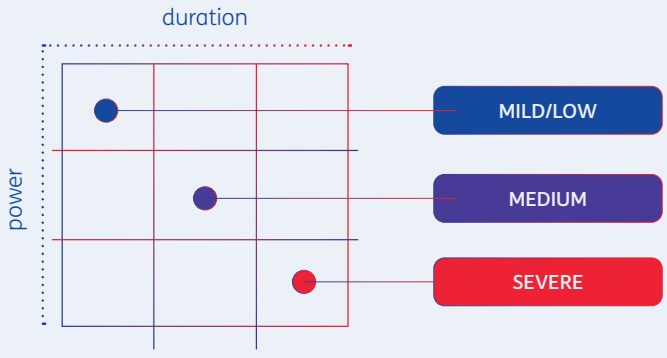
Also, the effects caused may contribute to differentiating the attacks. However, by considering the sole variables of intensity and duration, we can represent this transformation on a map of attack severity. By crossing these two features, we can highlight different reference areas (mild, low, medium and severe attacks), This enables us to visualise the growth of the phenomenon, its trend and the direction in which the attacks are oriented.

The historical analysis of data gathered since 2019 shows that the focal point has shifted from a mild/low severity area to a more intermediate one due to the increase in power and duration of the DDoS attacks.

However, the average duration tends to decrease, slightly changing the dynamics of the focal point variation that has been observed in recent years.

THE SEVERITY MAP

The crossing of two variables defines a space where we can allocate each attack according to its duration and power and carry out several analyses of the trend of event trends over time.

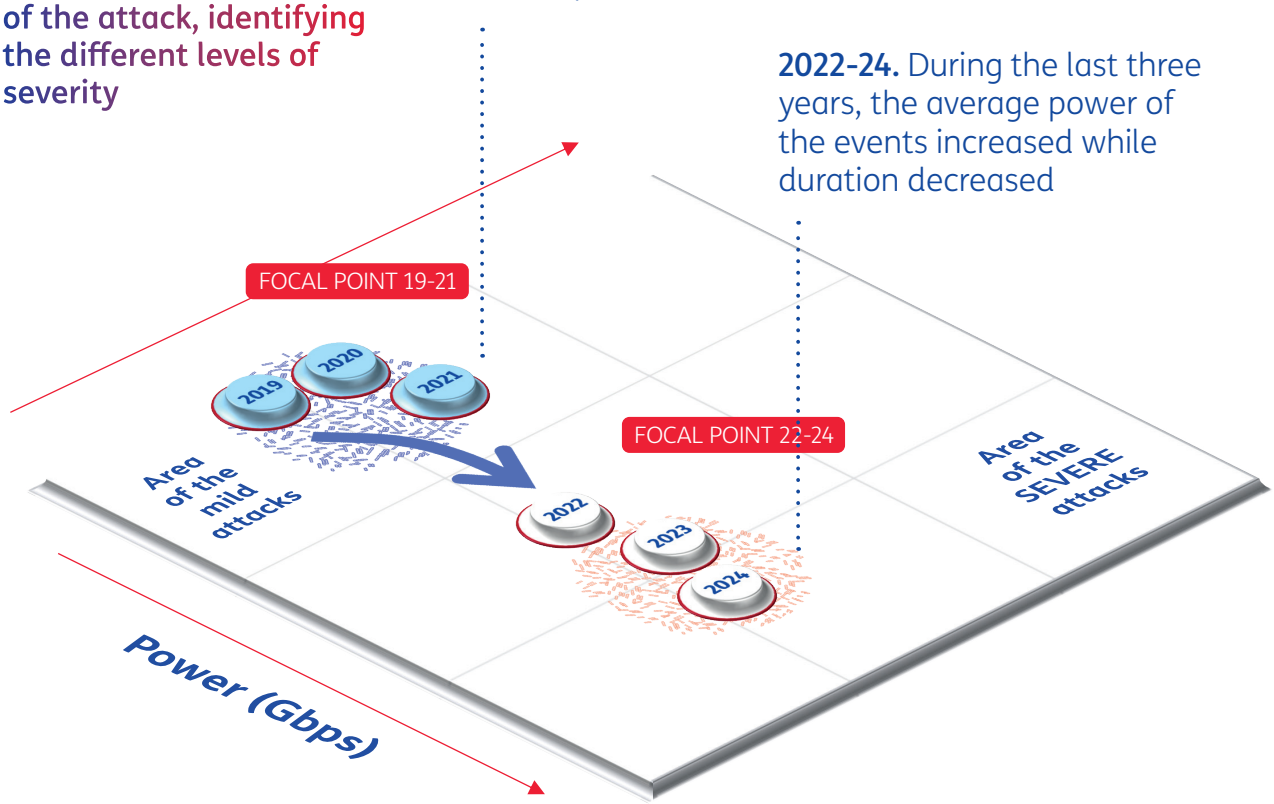


THE SEVERITY MAP
2023 vs 2024

DDoS events can be classified according to the duration and power of the attack, identifying the different levels of severity

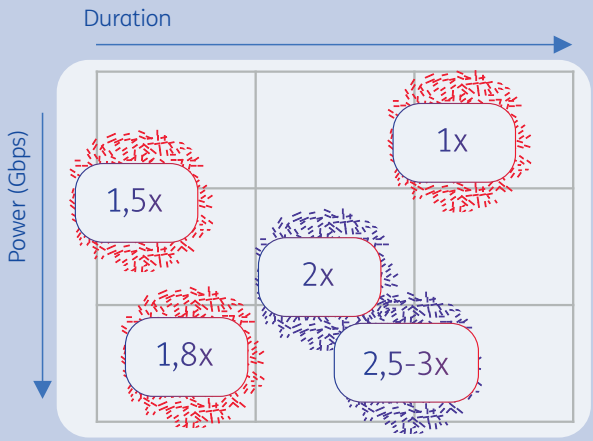
2019-2021. From 2019 to 2021 the majority of DDoS events has low intensity (between 2 and 4 Gbps) and lasts less than 30 minutes

2022-24. During the last three years, the average power of the events increased while duration decreased



2023 VS 2024

How weight changes per single severity area



The above shows that between 2023 and 2024, the number of high power and short duration phenomena almost doubled, while the low intensity and long duration events essentially did not change. The most significant increase is recorded in the high intensity and medium duration 2-3X) events

Severity growth increases the need **for mitigation**

THE MAXIMUM SEVERITY EVENTS INCREASED BY FOUR TIMES IN FOUR YEARS

The shift of the focal point towards an intermediate area is a natural consequence of the trends observed and is more clearly evident when we consider the trend of the maximum severity attacks over the last few years. In 2020, considering all the attacks within the severity area, they accounted for 6% of the total, in 2022 their incidence reached 12%, doubling the relevant weight in two years. In 2024 the share reached 26%.

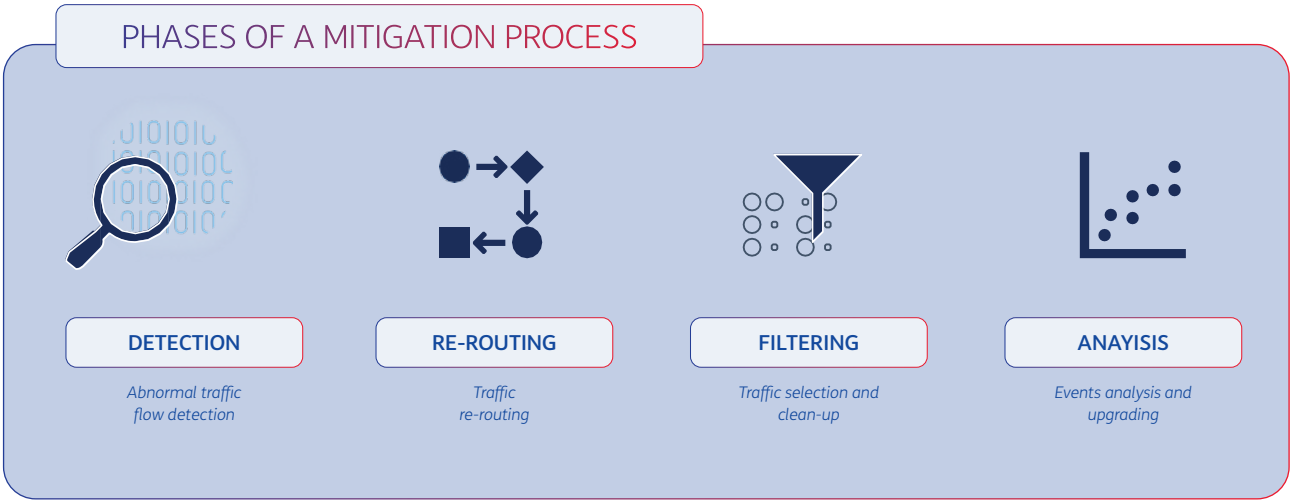
In other words, maximum severity events grew by more than four times in four years.

During the same period, the medium severity events reaching 22% of the total more than doubled. Overall, medium and high severity DDoS events represent nearly half of the total (against 16% in 2020).

THIS REQUIRES MORE EFFORT IN TERMS OF PREVENTION AND MITIGATION

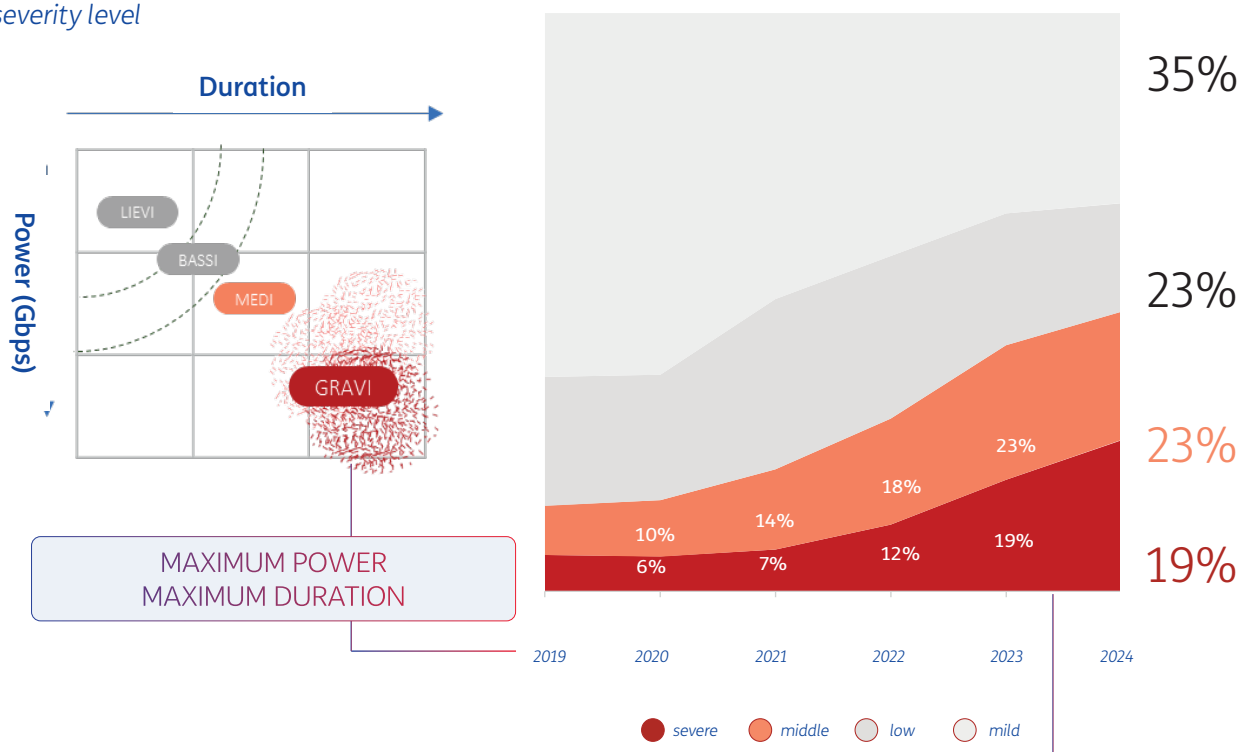
As attack capabilities increase, there must be a corresponding focus on defence capabilities. The ongoing transformation of cyber-attacks attempts, DDoS attacks included, requires a constant update of technologies and systems of prevention, detection, mitigation and response, so as to ensure protection and the continuity of activities by businesses, PAs and citizens.

The growing power of DDoS events over the last few months has required an increasingly intense mitigation activity to ensure a perimeter of defence equal to the growth and intensity of the attacks. In fact, in 2024 the mitigation events were more than three times those of 2020.

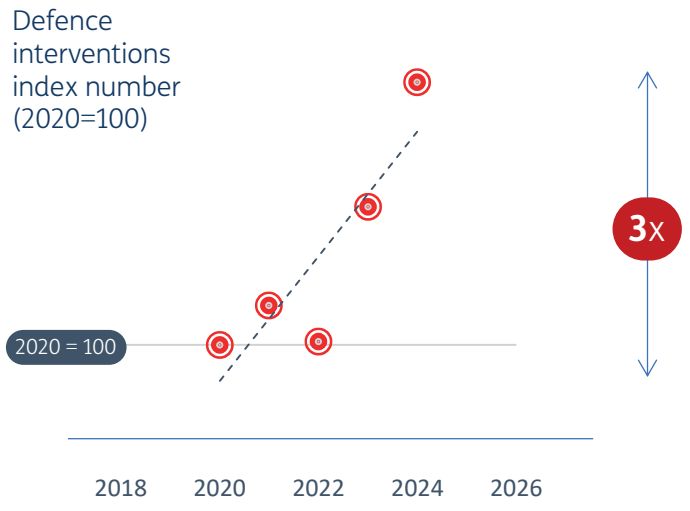


2023 (High and very high) **SEVERE ATTACKS TRIPLED COMPARED TO 2020**

Attacks % per severity level



THE NEED FOR INTERVENTION INCREASES



Given the intensity of the attacks, the need for intervention has more than tripled compared to 2020

DDoS Attacks, **opportunistic** strategies

DDoS attacks strike without distinction to generate damage and confusion, especially when they are launched with non-extortion purposes. In fact, some segments are hacked more than others simply because some «parts» of the system may be affected more easily and through this action the entire system is weakened. The strategy of the attack is often opportunistic and may vary over time based on several factors related to the features of the system, to circumstances and to opportunities deriving from the innovative techniques.

ALMOST 8 OUT OF 10 EVENTS DETECTED ARE DIRECTED TOWARDS "HOME USERS"

We distinguish between DDoS attack attempts aimed at households (i.e. private individuals in the context of non-professional activities) and those aimed at organisations, such as companies and institutions. About 3 out of 4 DDoS events that were detected in 2024 were directed at "Home Users", households and individuals. This share, in the five-year period 2020-2024, shows various fluctuations around an average value of 78% of the total. DDoS events targeting businesses and institutions account for 23% of all recorded cases in 2024

THE INSTITUTIONAL SECTOR SHOWS THE GREATEST GROWTH IN DDoS EVENTS. AMONG BUSINESSES, PROFESSIONAL SERVICES IS THE MOST TARGETED.

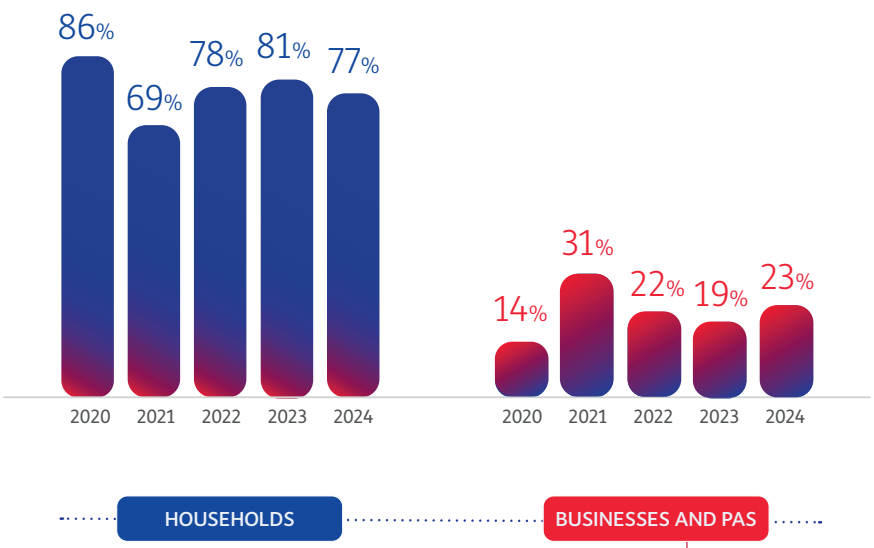
It is clear that the large volume of events addressed to the "Home Users" target does not allow for a clear observation of the dynamics affecting the other targets. Excluding this component, a significant increase in DDoS events against central and local Public Administration (PA) can be observed, with a growth from 1% to 42% of the total "non-Home Users" cases. At the same time, the financial sector recorded an increase from 3% to 14%, while defence went from 4% to 6% and the media from 1% to 2%. In contrast, professional services show a decreasing trend from 36% to 17% of DDoS events, although they remain a target of interest for attackers. Professional services are the most affected target in 2024 if we exclude institutional targets, followed by the financial and telecommunications sectors.

This change in attack trends suggests some considerations. On the one hand, the evolution of the geopolitical context puts targets that are considered representative of the country under fire, making them preferential targets for DDoS attacks. On the other hand, the evolution of cybercriminals' attack directions is becoming increasingly diversified and not always predictable and this increases the need for organisations to adopt increasingly advanced and effective security measures to protect their digital infrastructures.

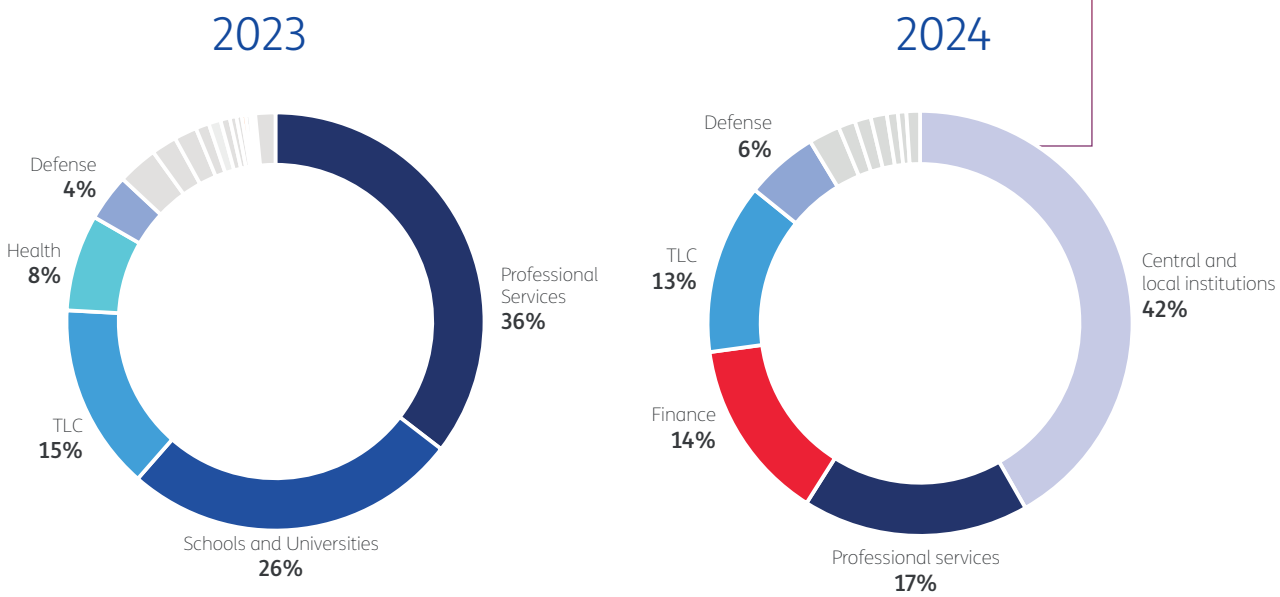
IN 2024 THE EVENTS AIMED AT BUSINESSES AND PAs REPRESENT JUST OVER 20%
of the total

DDoS attacks may have different motivations: opportunistic reasons, acts of digital vandalism, unfair competition, political activist movements, ordemonstration of power by hacker groups. The large number of events affecting the institutional sector suggests a potential correlation with the geopolitical context.

% of DDoS events aimed at businesses and households



Allocation of DDoS events aimed at businesses per sector



RANSOMWARE
Attacks

In the last few years, ransomware has become one of the most devastating attacks, targeting organisations of all sizes all over the world. Technically, it is a situation where the attackers take control of the asset of a target and demand a ransom in exchange for restoring the situation.

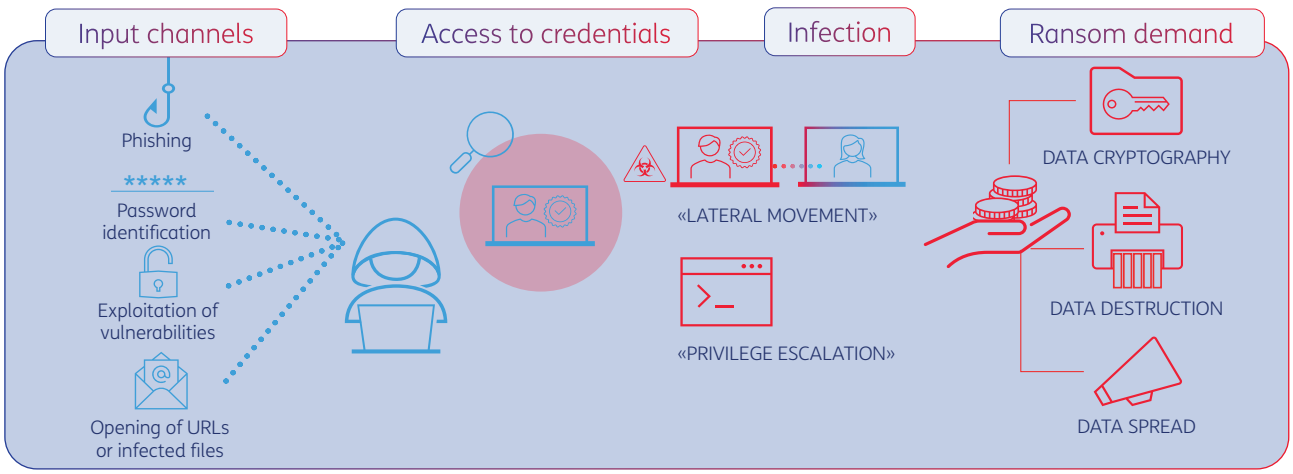
The most structured Ransomware groups activate «double extortion» models: to put pressure on the victims they employ the blockage/destruction of resources, together with a preventive exfiltration of data and information that, if released online, can cause different types of damage (criminal, legal, competitive...).

The increase in volumes is also due to ransomware-as-a-service, a model in which this type of attack is put on the market and offered as any other service.

A ransomware attack follows several phases:

- The exploitation of a system's weaknesses (phishing, identification of weak passwords, vulnerabilities, opening of URLs or infected files), for example, enables the attacker to penetrate the networks and to move freely in their environment, moving to other computers or penetrating accounts with enhanced privileges.
- Once the weakness is identified, the threat is carried out, warning the attacked subject of the impairment of its systems, blocking the access to the affected digital resource with consequent ransom demand.

Below we show the data collected by our Threat Monitoring system during the year. The rates do not represent the complete scale of the phenomenon, but merely its visible part. Unfortunately, despite the Authority's recommendations to the contrary, the affected actors give in to ransom demands and this does not facilitate the gathering of information. Much information is taken from the claims of the Ransomware groups.



RANSOMWARE attacks
Recap **2024**

In 2024 there were more than 5,200 ransomware claims at the global level, an increase of 12% compared to the previous year. Nearly half of the total were aimed at the United States

146

revindicated ransomware attacks towards Italy (around 3% of the total globally)

The sectors most affected by Ransomware attacks

Manufacturing
Professional Services
Technology
Commerce

Italy is the second EU country per ransomware attacks

behind Germany (168). As to the whole of Europe, the UK is the most targeted country (262)

42 **active attackers** in Italy during 2024

RansomHub, Lockbit and Black Basta were the most active groups in our Country

The Italian regions most affected by ransomware attacks were **Lombardy, Latium, Emilia-Romagna and Piedmont**

Ransomware attacks: Italy is the second EU country **per number of attacks**

THE RANSOMWARE PHENOMENON IS DIFFICULT TO MONITOR

To carry out an analysis of the ransomware phenomenon is particularly complex for different reasons:

- first, there is an inherent difficulty in the gathering of data, as the attack is not always followed by the reporting of the affected subject despite the recommendations and the obligations which are gradually being defined to deal with this phenomenon.
- In other cases, the reporting comes late and the claims of the criminal groups are not always to be relied on.

This leads to inconsistencies among the collected data and increases the perception to be facing a phenomenon of which we see a single part but not its entirety. A «tip of the iceberg» effect typically inherent to other criminal or illegal phenomena.

MORE THAN 5,200 RANSOMWARE ATTACKS IN 2024, MOST OF THEM TOWARDS THE USA. ITALY FACED 146 EVENTS (3% OF THE TOTAL)

The monitoring system implemented by the Intelligence Threat TIM Group recorded more than 5,200 ransomware attacks at global level during 2024, including 146 in Italy (compared to 176 in 2023).

The country most affected by ransomware attacks is the United States, with more than 2,650 incidents reported. In practice, nearly one in two attacks concerned U.S. businesses. Italy is in fifth position in the ranking of the countries affected by these events, ahead of Germany and followed by France, Brazil and India.

Considering the European Union as a whole, the ransomware attacks are 835, i.e. around 16% of the total. Overall, in the last three years observed, we detected 389 incidents in Italy, which is equal to 18% of the total reported by other EU countries.

THE GLOBAL MONITORING EFFORTS enabled to detect **MORE THAN 5,200 RANSOMWARE ATTACKS**

Focusing on the groups responsible for ransomware threats, 88 have been definitely identified based on their claims, 42 of which are active in Italy.

THE VOLUME OF RANSOMWARE ATTACKS
In Italy, the EU and the USA

88
attackers
globally

42
active
in Italy

THE U.S.A.

is the country most affected by claimed ransomware attacks.

2,640
attacks

51%
of the total

THE EUROPEAN UNION

represents the second target at global level

867
attacks

16%
of the total

ITALY

is the second EU country per overall ransomware attacks

146
attacks

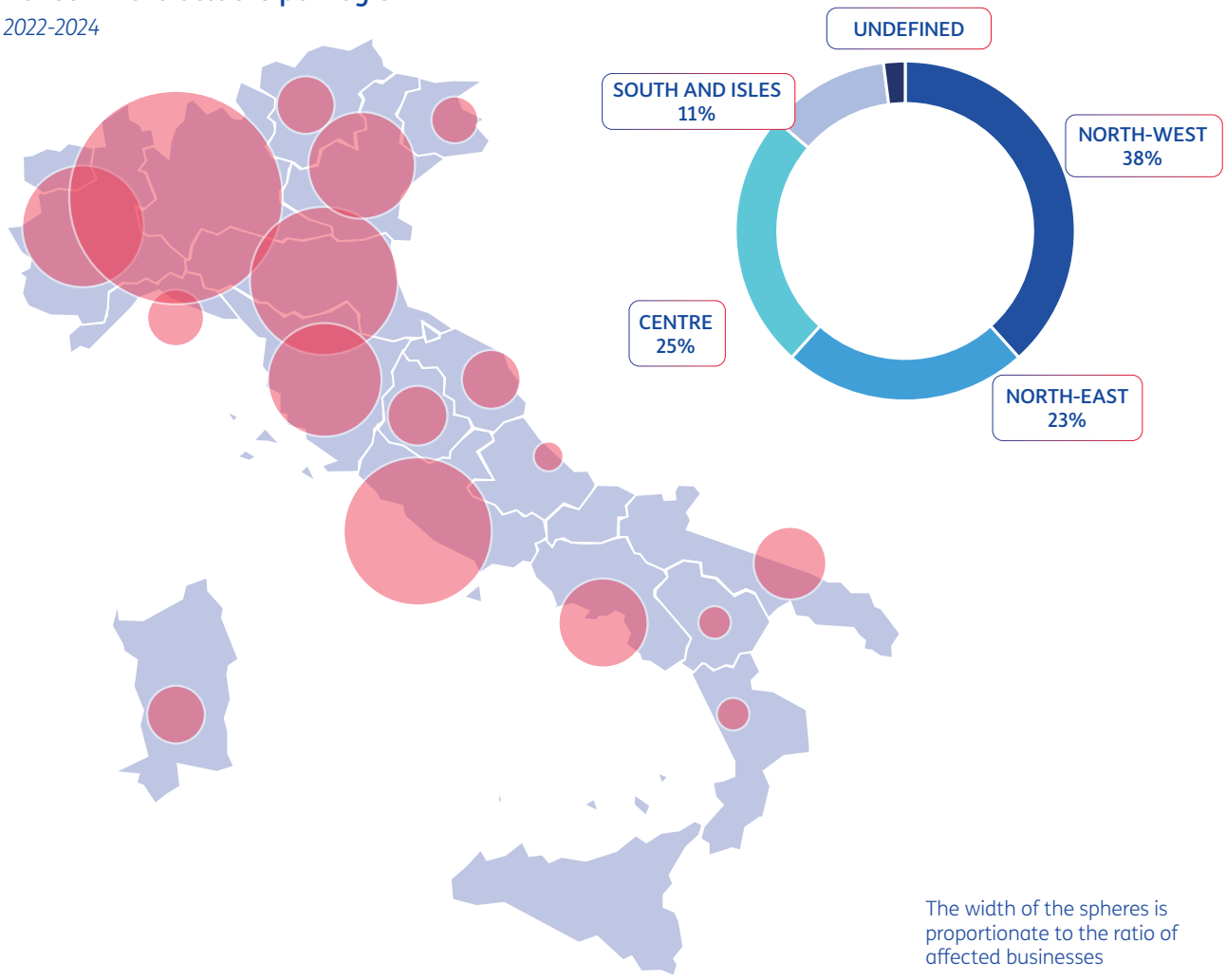
~3%
of the total

Ransomware attacks: The North-West is **the most targeted**

Based on the data collected on ransomware incidents, we can account for the geographic differences specific to our country. A significantly greater exposure to the phenomenon is evident in the North-West area of our country (38% of ransomware incidents in 2024), while the South and Islands represent a much smaller share (approximately 11% of the total). Lombardy is the region with the highest number of incidents in 2024 (40), followed by Latium, Emilia-Romagna and Piedmont. No incidents were detected in Molise and Sicily. The unique nature of ransomware prevent us from fully determining whether these differences are solely due to the relevant production structures of these areas or to differences in reporting the phenomenon.

Ransomware attacks per region

2022-2024



The width of the spheres is proportionate to the ratio of affected businesses

The most targeted sectors: professional services and **manufacturing**

No sector is immune, but we can identify some peculiarities when analysing the impact of ransomware attacks across different areas of our economic system.

In particular, the service industry seems more likely to attract ransomware attacks, while the secondary sector seems less exposed.

Attacks allocation per sector

total % of the detected incidents detected on a three-year period

1%

THE PRIMARY SECTOR IS STILL IN SECOND ROW

41%

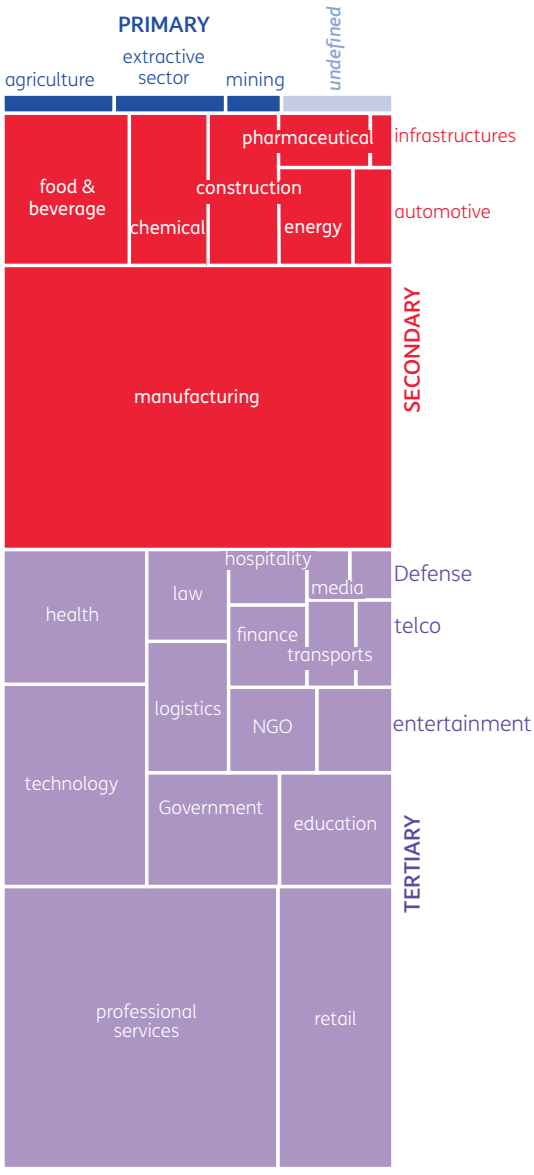
CONCENTRATED ATTACKS MOSTLY TARGET MANUFACTURING

Approximately 41% of ransomware events in the three-year period from 2022 to 2024 targeted the secondary sector, with 39% occurring in 2024. This sector is the most affected overall, with manufacturing companies being the target of roughly 26% of ransomware attacks during the three-year period, and a growing incidence in 2024 (30%).

58%

THE TERTIARY SECTOR IS MOST AFFECTED BY RANSOMWARE ATTACKS

The tertiary sector is the most affected, especially because it includes businesses that manage highly sensitive information such as banking or insurance data or medical records. The more valuable the information, the more attractive it becomes for ransomware. Moreover, the presence of large commercial networks with branches, offices and partners increases the scope of attack. In the three-year period 2022-2024, approximately 58% of events involved the tertiary sector, with a slightly higher incidence in 2024 (59%). The most targeted sector is professional services, with an average of 18% during the three-year period, and about 22% in 2024.



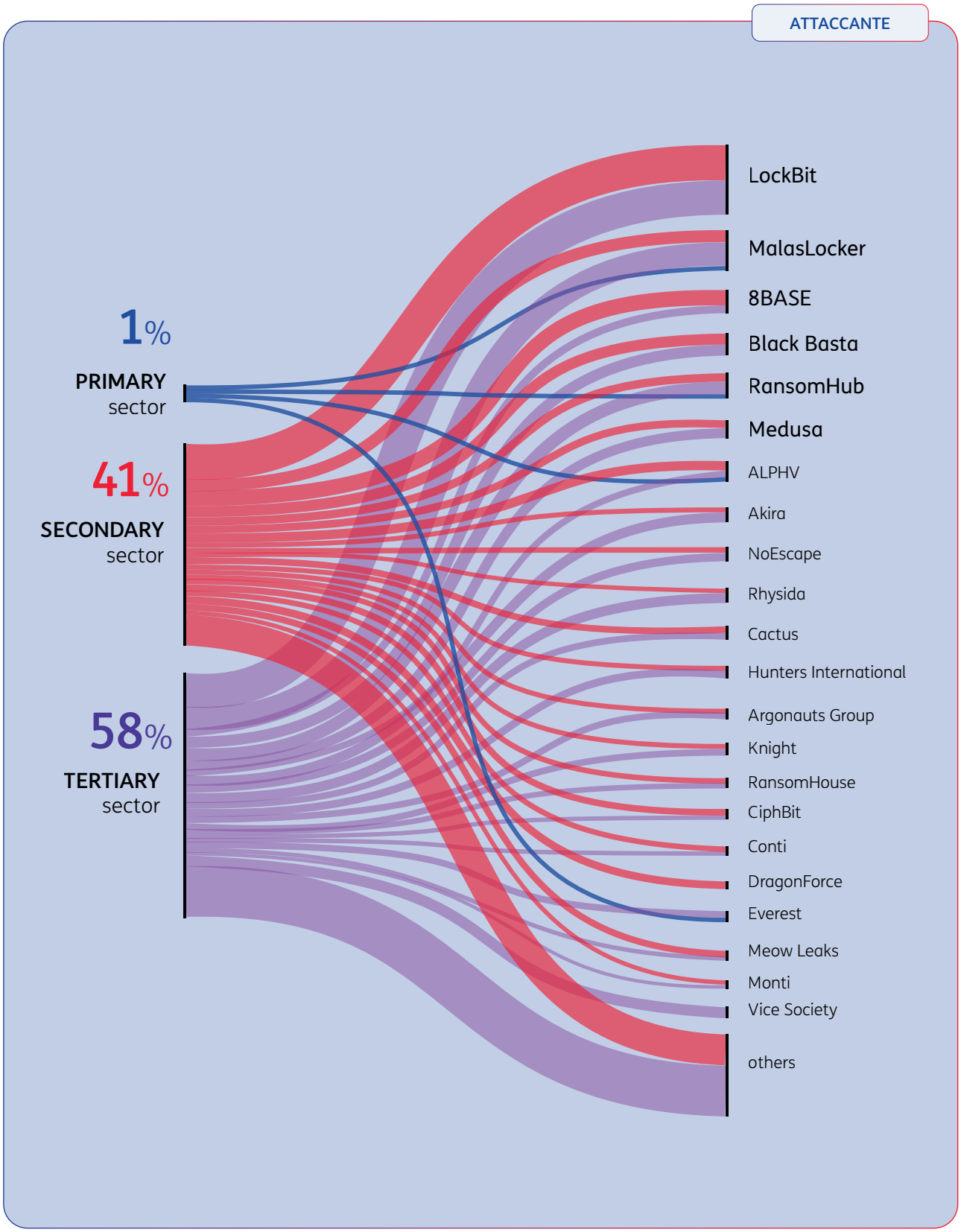
The activity of hacker groups: the importance of **RaaS**

During 2024, 42 hacker groups that brought ransomware threats to Italy were identified, out of a total of 88 attackers found globally. Among the groups that claimed ransomware attacks in Italy, the most active have been: RansomHub (18 cases), Lockbit (12 cases), 8BASE (11 cases) and Black Basta (10 cases). In the three-year period 2022-2024, Lockbit was responsible for 21% of detected cases, followed by MalasLocker (9%) and Black Basta, 8BASE and RansomHub (around 5%). The timeline of actions taken by these attackers shows significant differences. Lockbit made claims throughout the relevant period, with more intense activity during 2022-2023 and a decrease in activity during 2024. MalasLocker's activity seems to be concentrated in May 2023. Instead, Black Basta, 8BASE and RansomHub were more active throughout 2023-2024. These actions often seem to be driven by opportunistic reasons and no specialisations are identified in specific sectors or areas. However, based on the claims collected, while Lockbit and Black Basta distribute their actions quite equally across all sectors, 8BASE appears more focused on the secondary sector (80% of ransomware between 2022 and 2024), and RansomHub is more inclined towards attacks on the tertiary sector. And yet, when assessing these results, we have to consider that in recent years, the growth of some groups is also due to the spread of Ransom-as-a-Service (RaaS) models, a cybercrime business model in which a gang sells its ransomware code to other hackers, who then carry out ransomware attacks. Clearly, the more a group launches RaaS solutions, the more RaaS increases its weight in the rankings. According to a 2022 report by Zscaler, 8 of the 11 most active ransomware variants were RaaS variants.

HOW THE RAAS MODEL WORKS

The RaaS works the same as a legitimate Software-as-a-Service business model. The ransomware developers (RaaS operators) create ransomware tools and infrastructure and prepare RaaS kits to be sold to other hackers, the so-called RaaS affiliates. It is easy to understand why the RaaS model is so popular with cybercriminals. In fact, it lowers the level of knowledge needed to engage in cybercrime, enabling threat actors with limited technical skills to carry out cyber-attacks. RaaS, moreover, is mutually beneficial: the hackers can profit from the extortion without developing malware and the ransomware developers can increase their profits without having to attack the networks manually. The RaaS kits are advertised on the dark web forums where some ransomware operators actively recruit new affiliates. Once acquired the kit, the affiliates may count on a customer service, and in some cases, on ancillary services as well (support forums, ransom demands writing services, assistance with the negotiations, etc.). The business models can vary from service monthly rental to profit sharing (ransom share).

DISTRIBUTION OF THE ATTACKS
per industrial sector and per attacker



MALWARE
campaigns

Malware distribution campaigns represent a concerted effort to propagate malicious software, also known as malware (MALicious softWARE), through various channels to compromise computer systems, networks and devices, and through different means (virus, worm, trojan, spyware etc.), each with its specific operating modes.

Frequently, these campaigns exploit system vulnerabilities or use social engineering techniques, infected e-mail attachments, hacked websites and corrupt links to spread malwares. The purposes for which Malware campaigns are launched are different, including:

- gaining unauthorised access to devices to exercise control over them.
- Stealing confidential information (passwords, bank account log-ins, etc.)
- Spamming or other malicious activities through the compromised devices.
- Encrypting or damaging customers' files, occasionally demanding a ransom for their recovery (ransomware).

This type of attack can be launched globally, or it can affect specific targets (sectors, countries).

The most active in Italy during 2024 belong to these categories:

- **Keylogger:** malware designed to secretly record the keystrokes on a computer or a mobile device.
- **RAT:** the Remote Access Trojan or RAT installs itself on a computer, a mobile device or other equipment, and opens a breach enabling the attackers to control the infected machine from afar.
- **Infostealer:** malware infecting computers and devices to steal data or information.
- **Downloader:** designed to download and install malicious software. They pave the way for other malware.
- **Loader:** software that loads other malwares in memory.
- **Banking Trojan:** specifically designed to steal log-in credentials and sensitive information related to online banking and hack the account.
- **Compromised website:** this category indicates that compromised websites have been used to distribute or perform attacks.

MALWARE campaigns
Recap **2024**

168

malware campaigns

targeting Italy counteracted in 2024

In Italy the RAT Malwares (Remote Access Threat) were more prominent

This malware installs itself covertly, enabling the attackers to control the infected machine from afar

nearly **40%**

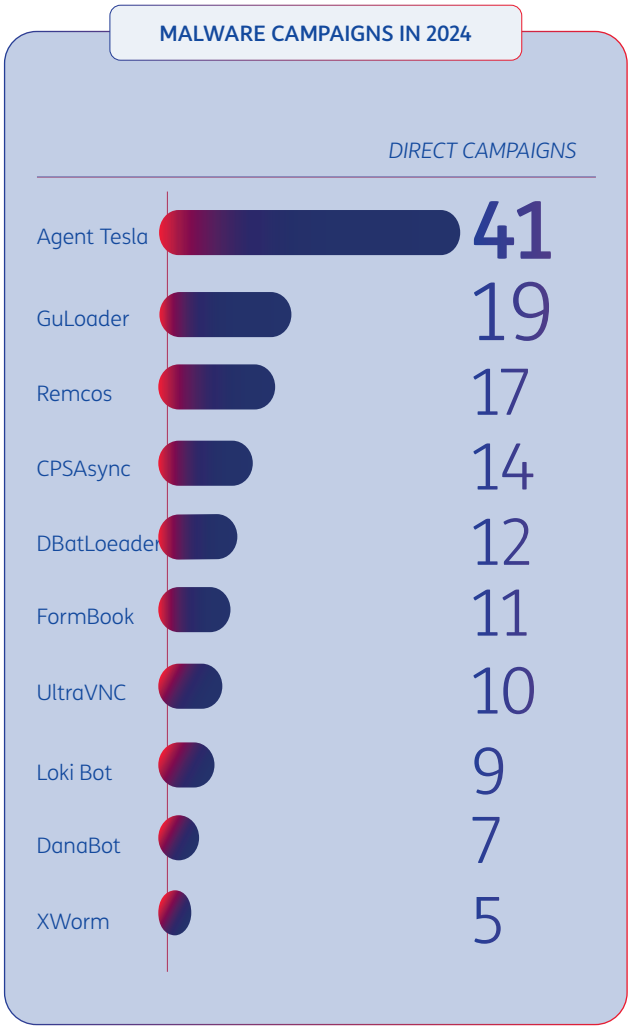
of malware campaigns targeting Italy are linked to **Agent Tesla** and **GuLoader**

Malware campaigns: more than 160 campaigns **targeted Italy**

The malware campaigns can be both global and aimed at specific countries, and the difference lies mainly in their purpose and scope. Global Malware Campaigns are launched indiscriminately with the aim of affecting as many subjects as possible. Often, these actions are intended to prepare the ground for other malicious activities (for ex., create an extensive network of compromised machines from which to launch DDoS attacks).

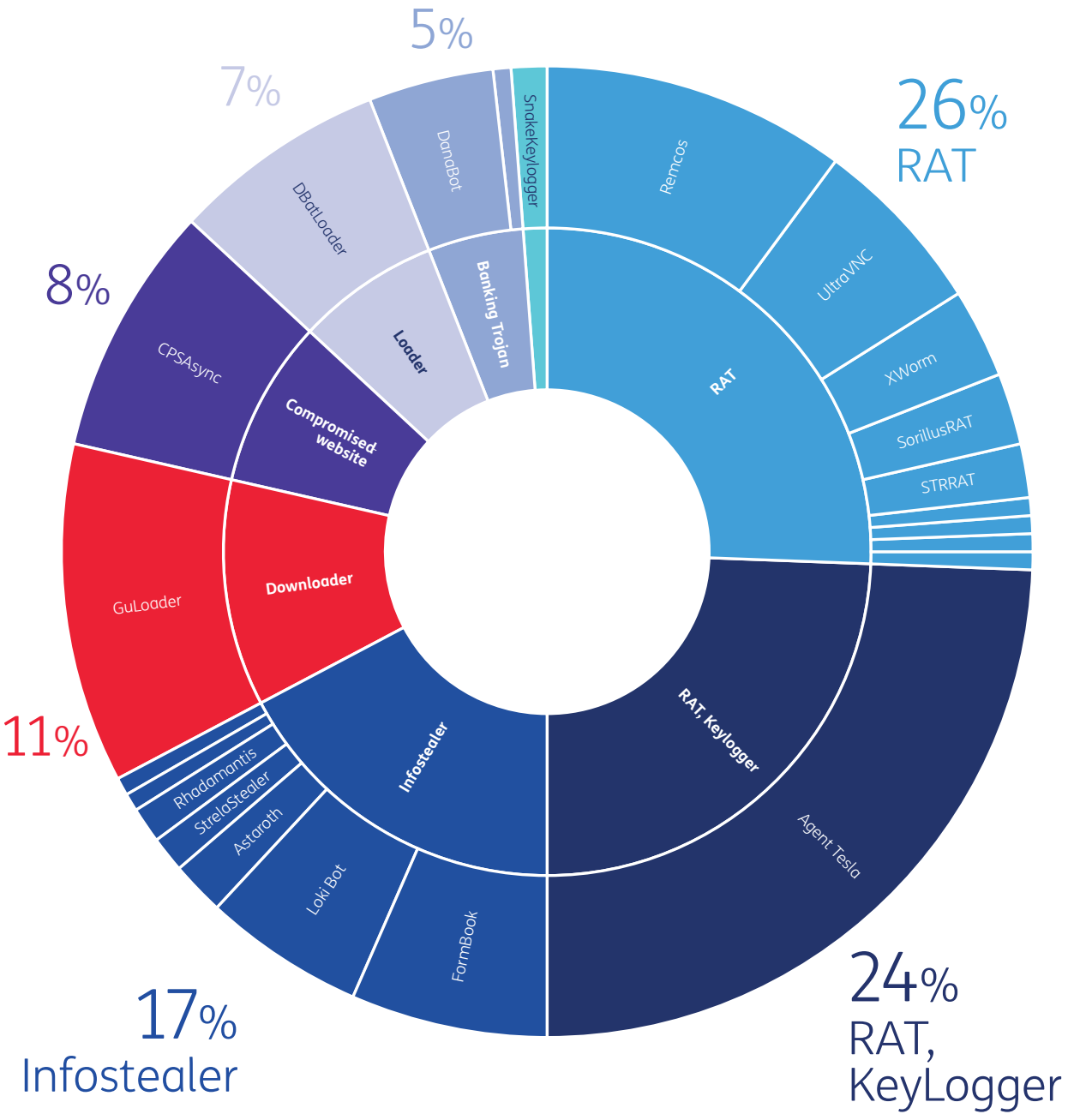
The targeted campaigns attack a given target both for opportunities (specific vulnerabilities), and to affect a Country deliberately (for ex., actions launched with political or cyberwarfare purposes).

During 2024, 168 Malware campaigns were identified and counteracted. Among direct campaigns, in 2024 the main malware threats were brought by AgentTesla (41 campaigns) and GuLoader (82 campaigns). These threats represent 36% of the malware campaigns specifically targeting our country.



MALWARE CAMPAIGNS
per typology

In 2024, just over one in four malware campaigns (26%) was of the RAT type. Agent Tesla had both RAT and Keylogger features and accounted for 24%, followed by Infostealer (17%) and downloaders (11%).



SECOND PART

Sector insights

A large part of the cyber-attacks detected targeted the consumer world, i.e. households and individuals. The most disruptive attacks, however, affected businesses, manufacturing and institutions, which are the most attractive targets and represent the heart of our analysis.

The attacks on these targets are more sophisticated and have significant repercussions, such as halting production, restoration costs, data loss, reputational damage and consequences on market positioning. For public bodies, service companies and institutions, the disruption of activities also affects citizens' lives, potentially compromising national security.

In this section we provide a «reading» of the data gathered per areas of attack. Knowledge is a fundamental element of cybersecurity and delving deeper into what is happening in the cyber world is the first step in defining defence strategies that can enhance the level of protection and resilience of systems.

01 **Sectoral sheets**
Recap data for the main sectors affected

02 **The most dangerous opponents**
Focus on the most active cyber groups during the last 3-year period

Levels of exposure
an **overview**

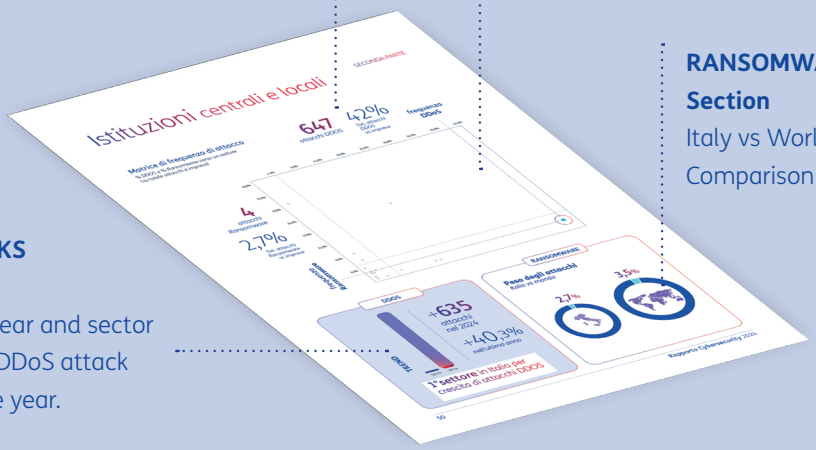
In the summary sheet, we report the relevant information for each of the sectors examined regarding the types of DDoS and Ransomware attacks. As we have seen, some sectors appear to be more generally exposed, while others are affected based on arising opportunities, specific vulnerabilities and targeted campaigns. In this regard, it may be useful to monitor what happens in one sector compared to others and highlight the trends of attacks over time. Another element which can emerge is a discrepancy between national and international levels. For the sectors which are typically more exposed, on average this discrepancy can indicate either a specific weakness or, conversely, a greater capacity for defense compared to the international average.

SECTOR SHEETS

Sector sheets are divided into four sections: a more general summary, one dedicated to DDoS, one to Ransomware, and an overview of attack frequency.

TOTAL VOLUMES
Number of DDoS and Ransomware attacks

Attack Frequency MATRIX
Sector positioning regarding DDoS and Ransomware threats



RANSOMWARE Section
Italy vs World Comparison

DDoS ATTACKS Section
Attack trend vs previous year and sector positioning in terms of DDoS attack variation over the year.

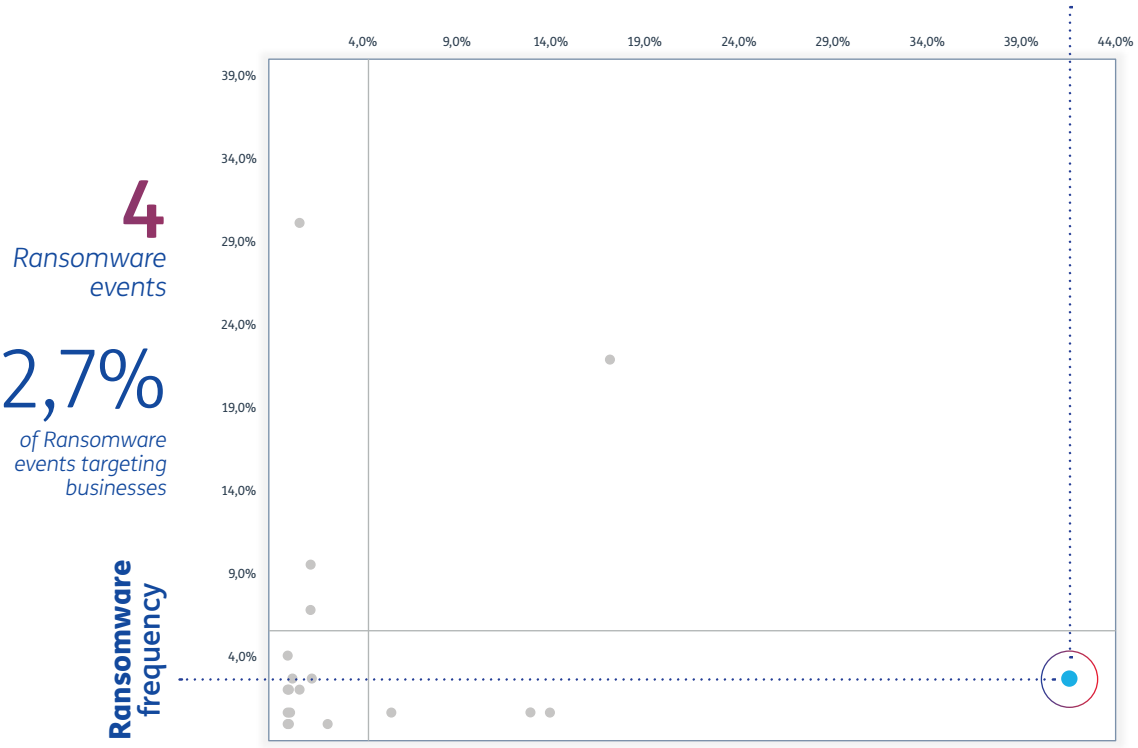
central and local Istitutions

Frequency MATRIX

of DDos and Ransomware attack-stargeting a given sector (% share of total attacks on businesses)

647
DDoS events

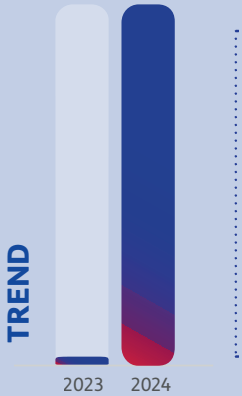
42%
of DDoS events targeting businesses



4
Ransomware events

2,7%
of Ransomware events targeting businesses

DDOS



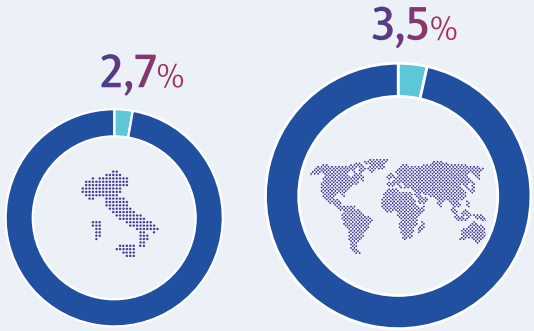
+635
events in 2024

+40,3%
during the last year

1st sector in Italy per growth of DDoS events

RANSOMWARE

Weight of the attacks
Italy vs World



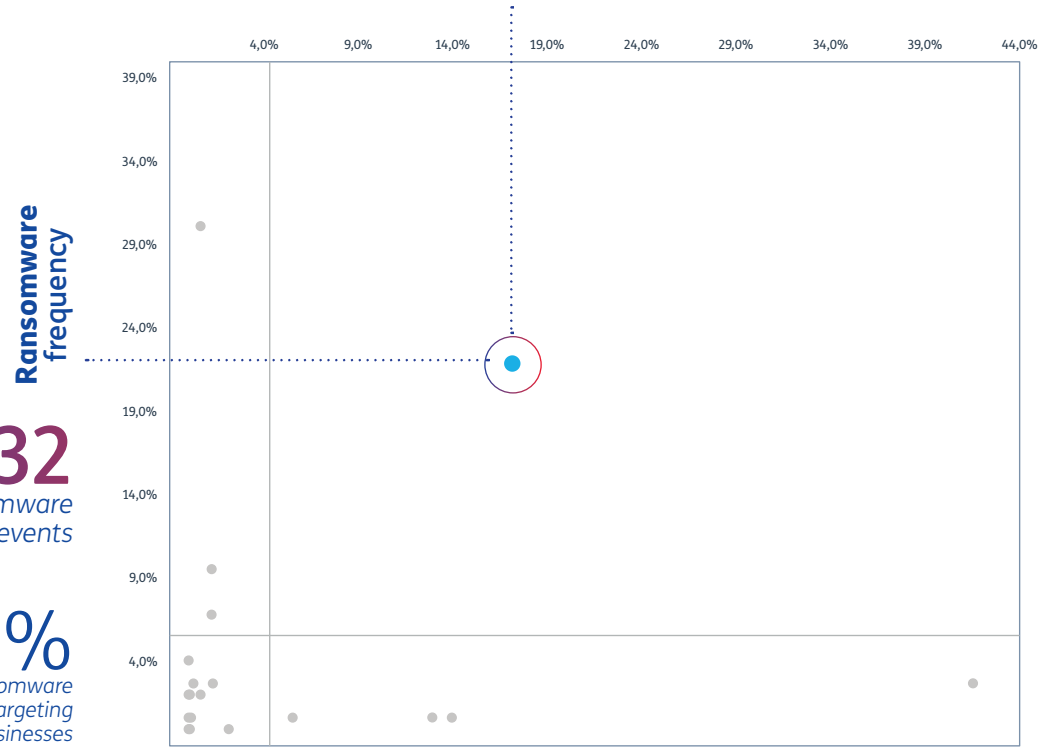
Professional services

Frequency MATRIX

of DDos and Ransomware attack-stargeting a given sector (% share of total attacks on businesses)

267
DDoS events

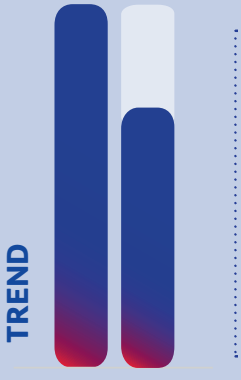
17%
of DDoS events targeting businesses



32
Ransomware events

22%
of Ransomware events targeting businesses

DDOS



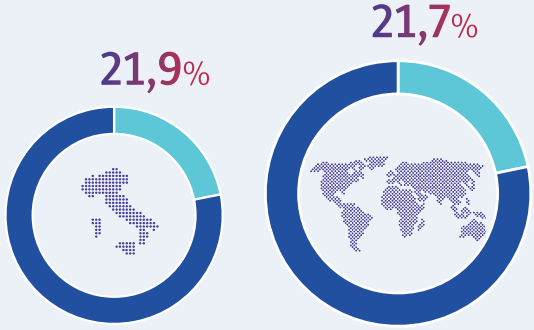
-75
events in 2024

-19,3%
during the last year

penultimate sector in Italy per DDoS events **contraction**

RANSOMWARE

Weight of the attacks
Italy vs World



Finance

Frequency MATRIX

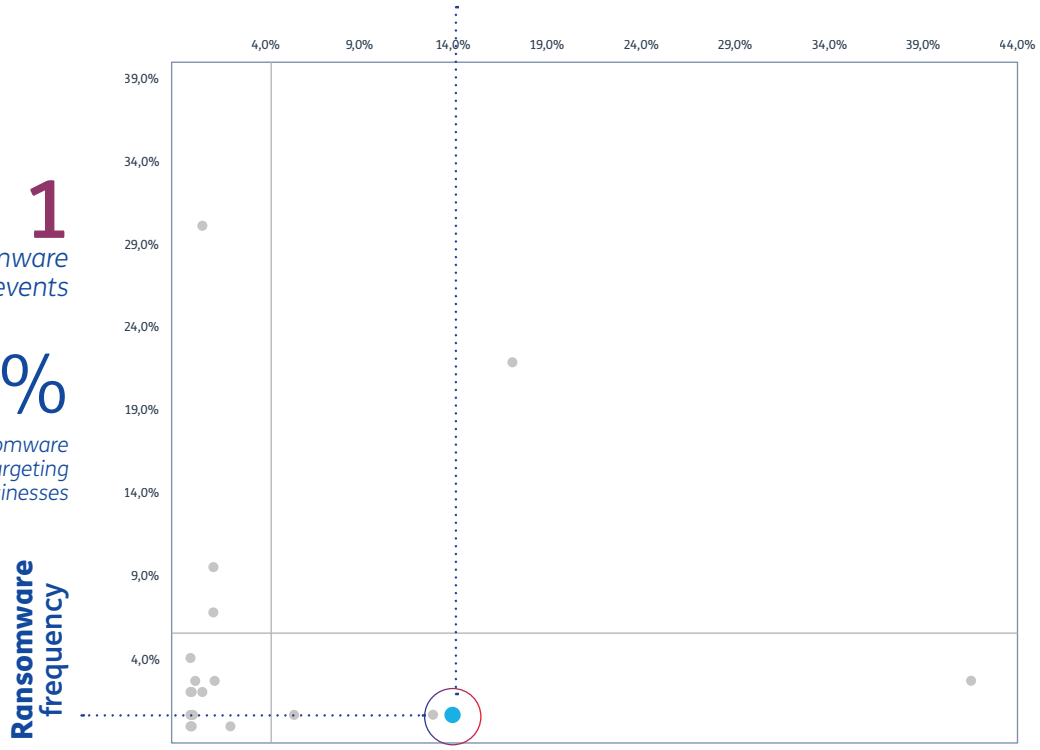
of DDos and Ransomware attack-stargeting a given sector (% share of total attacks on businesses)

217
DDoS events

14%
of DDoS events targeting businesses

1
Ransomware events

0,7%
of Ransomware events targeting businesses



DDOS

TREND

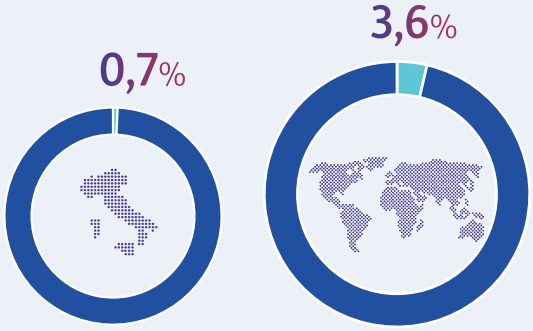
+187
events in 2024

+10,8%
during the last year

2nd sector in Italy per growth of DDoS events

RANSOMWARE

Weight of the attacks
Italy vs World



Manufacturing

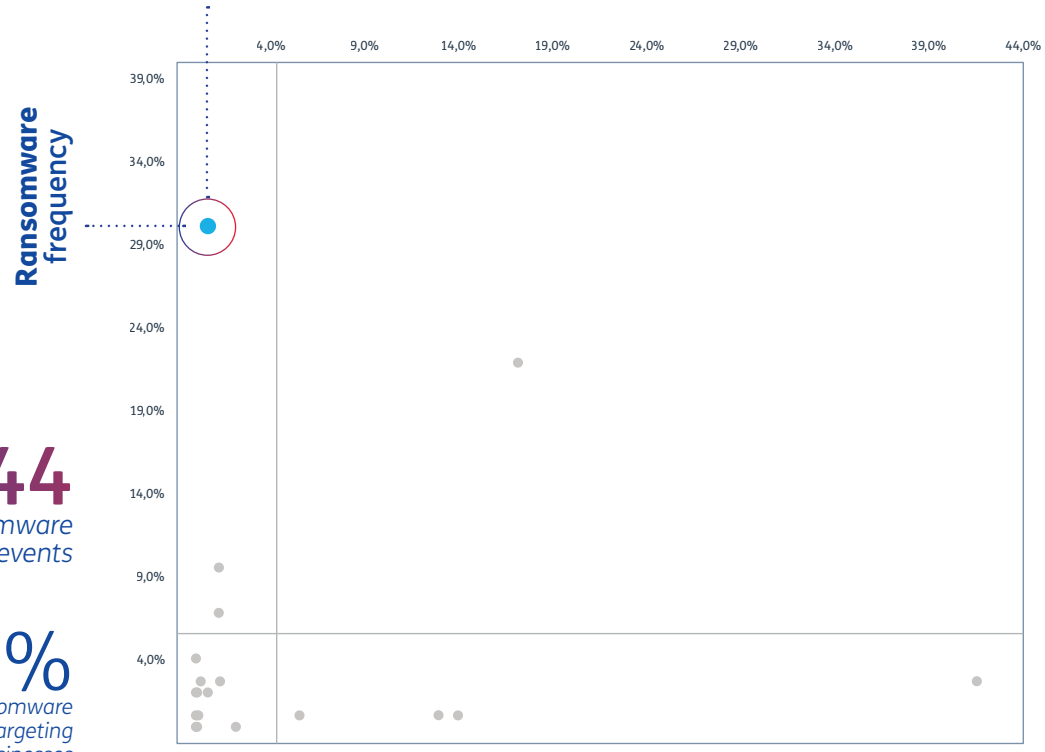
Frequency MATRIX

of DDos and Ransomware attackstargeting a given sector (% share of total attacks on businesses)

DDoS frequency

10 *DDoS events*

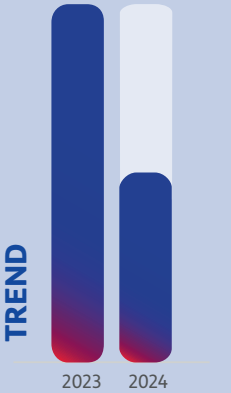
0,6% *of DDoS events targeting businesses*



44 *Ransomware events*

30% *of Ransomware events targeting businesses*

DDOS



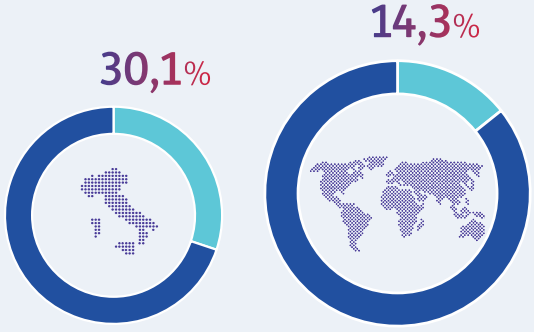
-9 *events in 2024*

-1,4% *during the last year*

contraction of DDoS events during the last year

RANSOMWARE

Weight of the attacks
Italy vs World



Retail

Frequency MATRIX

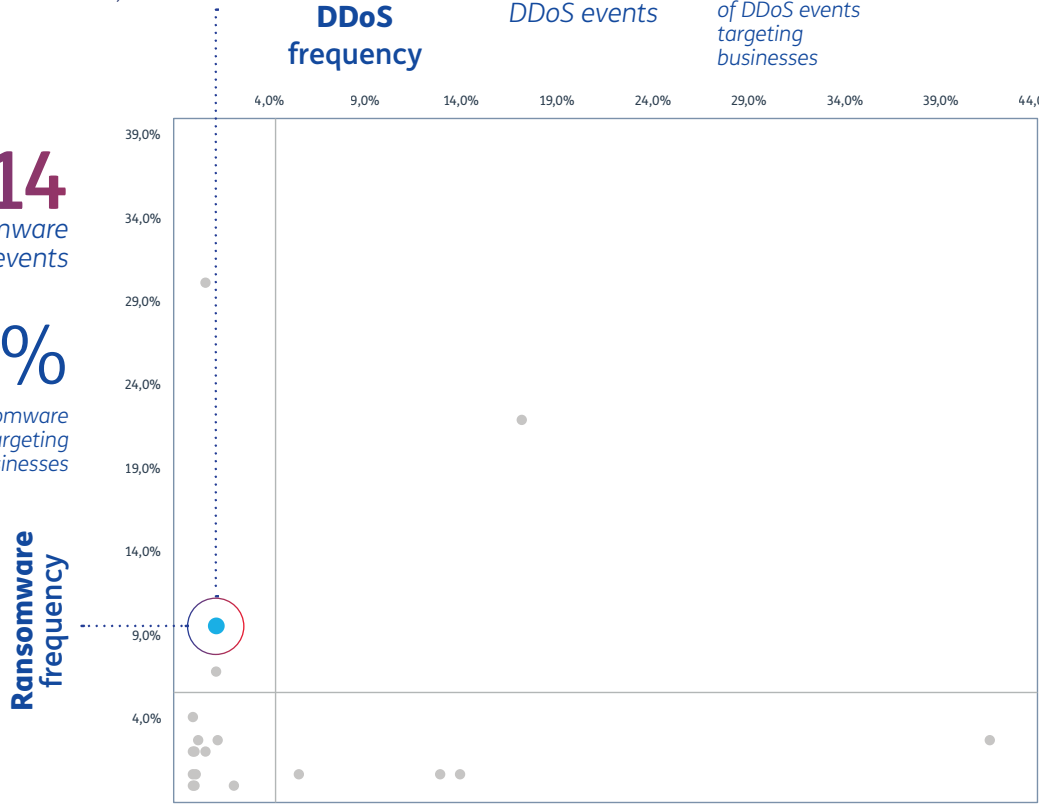
of DDos and Ransomware attack-stargeting a given sector (% share of total attacks on businesses)

19
DDoS events

1,2%
of DDoS events targeting businesses

14
Ransomware events

9,6%
of Ransomware events targeting businesses



DDOS

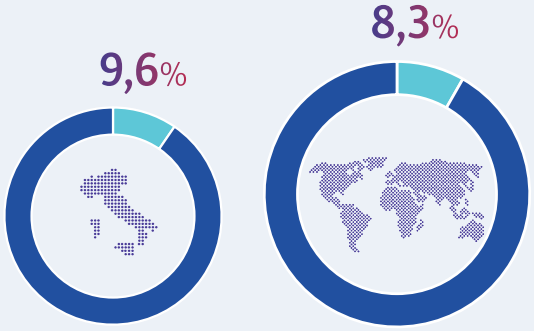
8th *sector in Italy per DDoS events in 2024*

together with the technological sector

*It is not possible to provide evidence of the growth trend in Commerce during the last year because, due to a revision of the categories, the data for 2023 are not available.

RANSOMWARE

Weight of the attacks
Italy vs World



The weight of the attacks in **all monitored sectors**

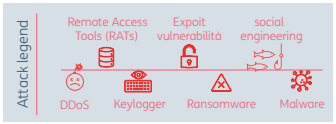
Frequency MATRIX

of DDos and Ransomware attackstargeting a given sector (% share of total attacks on businesses)

MAIN ATTACKERS PER TYPOLOGY 2022-2024

SECOND PART

State-sponsored



LAZARUS GROUP

ORIGIN:
North Korea, 2009

ALIASES:
Dark Seoul, Hidden Cobra, Unit 121, APT 38, PLUTONIUM, TAG-71, Andariel

PURPOSE:
Financing its own operations and the North Korean government

ATTACK TECHNIQUES

CNE (Computer Network Exploitation): Espionage

CNA (Computer Network Attack): destruction or tampering with computer systems.

- *Manipulation of accounts and access tokens;*
- *acquisition of Infrastructure (domains, servers, web services);*
- *automatic execution at startup or authentication;*
- *data interception (network traffic, web protocols, apps);*
- *data management and storage.*

TARGET

Wide range of sectors; preference for supply chain attacks that allow reaching a large audience of victims

SCARCRUFT

ORIGIN:
North Korea, 2016

ALIASES:
Kimsuki, KONNI, Sector05, APT 37, Velvet Chollima, Thallium, Geumseong121, Red Eyes, Reaper

PURPOSE:
Intelligence for the Reconnaissance General Bureau, North Korean Ministry of Defence

ATTACK TECHNIQUES

CNE (Computer Network Exploitation): Espionage

- *Manipulation of accounts and access tokens;*
- *automatic execution at startup or authentication;*
- *exploiting vulnerabilities in web protocols;*
- *audio capture;*
- *using command interpreters or scripting languages (Windows shell, Visual Basic, Python) to perform malicious operations.*

TARGET

High-profile targets in Asia, the US, Europe and Russia, with a preference for South Korea.

NONAME057

ORIGIN:
Russia, 2022

PURPOSE:
Pro-Russian Hacktivism; disrupting websites deemed anti-Russian and pro-Ukrainian

ATTACK TECHNIQUES

CNA (Computer Network Attack): destruction or tampering with computer systems.

- *Specific details on the techniques used for these attacks are not publicly available. In general, massive DDoS attacks are used.*

TARGET

Private and public businesses in countries that support Ukraine and NATO. Dedicated Telegram channel for claiming the attacks.

MAIN ATTACKERS PER TYPOLOGY 2022-2024
Ransomware

LOCKBIT TEAM

ORIGIN:
Russia, 2019

PURPOSE:
RaaS (Ransomware-as-a-Service)

self-financing

ATTACK TECHNIQUES

- *Credential theft;*
- *circumvention of debugging and code analysis systems and self-propagation;;*
- *adaptation to the specific configurations of the victims' corporate architecture;*
- *data encryption with ransom demand.*

TARGET

Wide range of sectors, without a specific target

MALASLOCKER TEAM

ORIGIN:
Unknown geographical area, 2023

PURPOSE:
Hacktivism;

Non-profit organization funding

ATTACK TECHNIQUES

- *Exploitation of vulnerability with unusual encryption method: use of particular algorithms;*
- *note with detailed instructions on how to make the donation - without specifying the amount - and provide the receipt.*

TARGET

Various sectors, Italian objectives highly targeted

BLACK BASTA TEAM

ORIGIN:
Russia, 2022

PURPOSE:
RaaS (Ransomware-as-a-Service)

self-financing

ATTACK TECHNIQUES

- *Using command interpreters or scripting languages (PowerShell, Windows Command Shell) to perform malicious operations;*
- *creating processes to execute malicious code in the background and maintain persistent access to the system;*
- *encrypting data with a ransom demand;*
- *circumventing debugging and code analysis systems;*
- *modifying the appearance of websites and internal apps.*

TARGET

Various sectors, including critical ones, mainly healthcare

Normative elements

As frequently mentioned, the cyberspace defence requires strong cooperation. The sharing of information and the establishment of common practices represent a very effective way to counter the threats coming from different actors who, in various capacities, bring cyber threats to citizens, businesses and national states.

As noted by the European Commission, «in a connected environment, a cybersecurity incident in one product can affect an entire organisation or a whole supply chain, often propagating across borders».

To structure a coordinated response at the European level, the EU tried to build a common frame of reference, modulating both the lawmaking and the more operational initiatives –from equipment certification to attack response processes -to facilitate a convergence process among national cyber-security systems, as carried out in other fields of common interest.
For this reason, it is essential to monitor the trend of the regulatory framework, which represents one of the stimulating factors in the national defence strategy.

Cybersecurity in EU
Assets and **rules**

The protection of the European digital spaces is an essential factor to enable the achievement of a complete digital economy. This is a highly complex goal which overlaps several fundamental aspects:

- **technological developments,** which proceed at very high speed and require a constant review of protection policies. For example, 5G, the development of Cloud platforms and the Artificial Intelligence represent new focuses in need of new solutions.
- **The developments of the geopolitical framework** call for the review of the cyber-defence perimeters, adjusting them to new situations, and for the review of common protocols and agreements. Brexit, for example, required negotiations to manage the transition from a common European defence framework to a more fluid situation.
- **The changes in consumption patterns**, such as the progressive take-up of electronic payment systems, carried out through API (application programming interface) solutions which facilitate the automated interchange of information between equipment and systems. This, on the one hand, simplifies payment but expands the chain of intermediaries and requires a review of the relevant regulation for fraud cases and the theft of sensitive information.
- **New social sensitivities,** which for example demand a greater attention to data usage and to the propagation outside the European perimeter, to ensure that the treatment and the management are in line with the EU principles and values.
- **The conjunctural phenomena,** often unpredictable, such as the Covid spread, which had – among others –the consequence of accelerating the society digitalisation process, with smart-working, distance learning, the eCommerce boom which opened new areas to be assessed and defended to ensure a more secure environment.

These and other phenomena require a constant review of the regulatory framework. Trying to summarise, to face these changes, the regulatory developments in cybersecurity resulted in several regulations, of which the most impactful for the TLC sector are as follows:

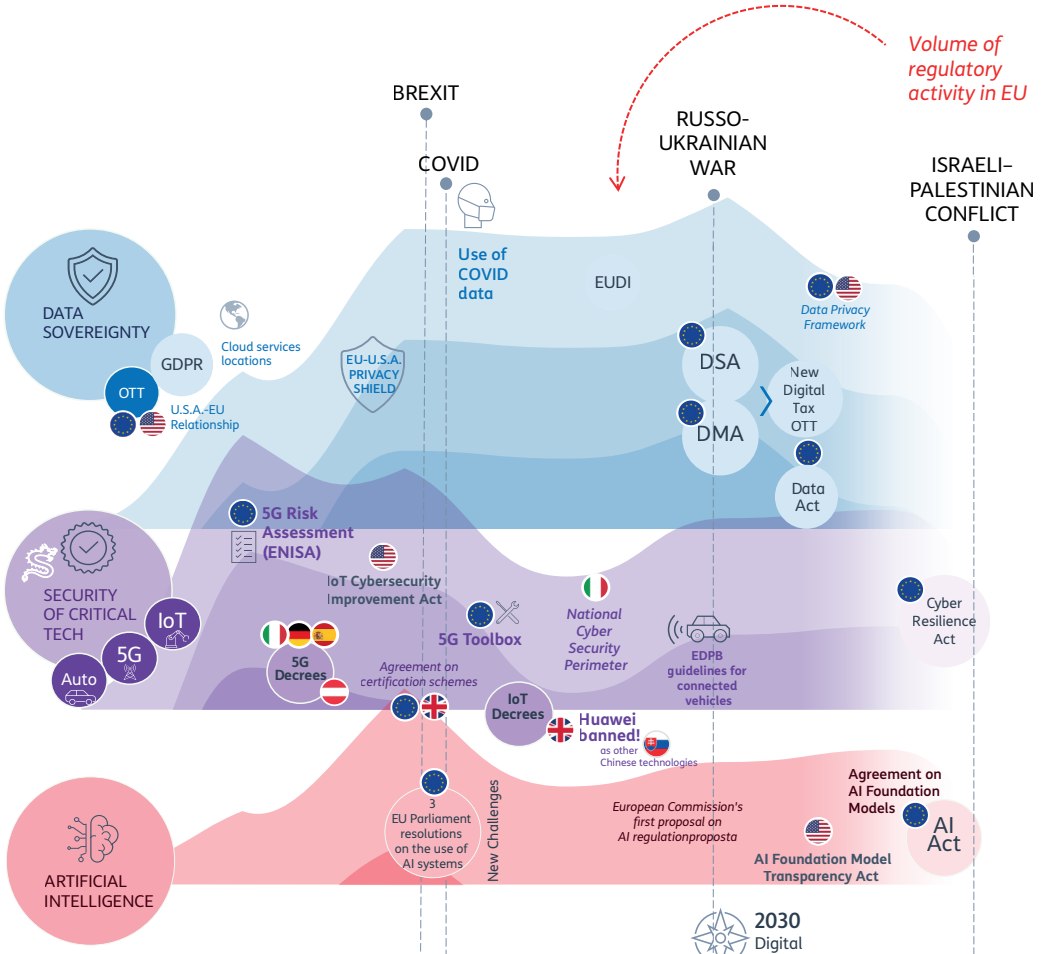
- The NIS Directive (2016)
- The Cybersecurity strategy (2017)
- The Cybersecurity Act - CSA (2019)
- The EU recommendation on the cybersecurity of 5G networks (2019)
- The new cybersecurity strategy (2020)
- The CER Directive (2022)
- The NIS2 Directive (2022, published in 2023)
- The Cyber Resilience Act – CRA (2024)

The first certification scheme based on the Cybersecurity Act and drawn up at European level is the European Common Criteria based cybersecurity certification scheme (EUCC). Currently there is a discussion on the cybersecurity certification schemes for

- Cloud services (EUCS)
- 5G networks (EU5G)

It is expected that the future certification schemes will be on Managed Services (recently included within the CSA application scope) and on digital identity portfolios (in compliance with the requirements of the European Regulation on digital identity, EUid). In addition to these more general acts, there are specific vertical regulations on more critical activity areas (such as the offer of financing and payment services, affected by the review of the Digital Operational Resilience Act or DORA).

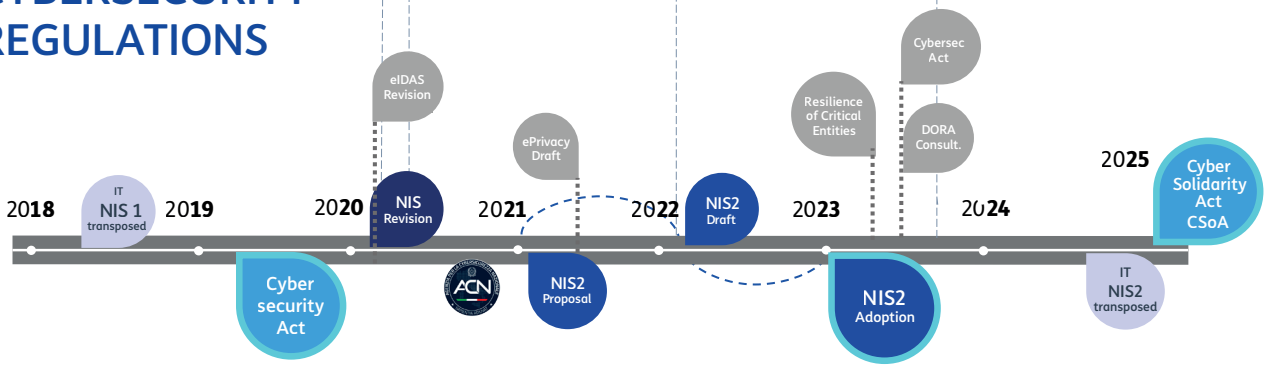
EVOLUTION OF THE EU REGULATORY FRAMEWORK



The EU Cybersecurity Certification Scheme on Common Criteria **EUCC**

Can be used to demonstrate compliance with the requirements of the Cyber Resilience Act

THE STAGES OF CYBERSECURITY REGULATIONS



Source: Cullen International, press news

From NIS to NIS2: a **fundamental** change

The first European horizontal measure to protect ICT security goes back to the Directive of the European Parliament and the Council dated July 6th, 2016, a joint legislative measure which aimed to increase co-operation among Member States and to create a first level of harmonisation regarding cyber-security: the **NIS** (Network and Information Security).

The Directive played a fundamental role in raising awareness on the cybersecurity risks and represented a guide for Member States:

- by defining **minimum security requirements** for the "essential services operators" (ESOs) and the "digital services providers" (DSPs) in strategic sectors [for ex. energy, transport, healthcare, digital infrastructure (i.e. IXP, DNS, TLD);

- by introducing **incident reporting obligations**, to adopt preventive measures and designate relevant national authorities such as the Italian ACN.

In Italy, the NIS was transposed into law by decree in 2018, and its process was intertwined with that of other regulatory measures aimed at creating a protected environment for the users of electronic communications services.

In 2018 the **European Electronic Communications Code** (EECC), transposed in Italy in 2021, extended the security measures for electronic communications networks and services present in the previous framework.

The scenario evolves extremely quickly, with an increasingly intense exchange of data in the cyberspace –also due to the pandemic: a regulatory review had already started in 2020 and **in 2022 all security measures had been transferred to the NIS** and the related EECC articles were repealed.

The 2022/2555 (NIS2) Directive was published in the OJ on 27th December 2022 and replaced the NIS Directive. The NIS2 aims to achieve two main objectives:

1. an **increased level of cyber-resilience** among public and private actors, also by extending the scope of application.

2. the **improvement of the collective levels of awareness and skills management** and response to cyber threats.

The Commission decided to maintain the regulatory Directive tool by adopting the principle of minimum harmonisation to ensure sufficient flexibility in the transposition of the measures at national level.

Hardware and Software providers do not fall within the NIS scope of application. The Commission is regulating these and other aspects through other tools, such as the EUCC certification, the new Cyber Resilience Act (CRA), regulation on connected products, or the European Artificial Intelligence Regulation (AI Act), the Digital Operational Resilience Act (DORA) related to the digital operational resilience of the financial sector, and the Critical Entities Resilience Directive (CER), related to the cyber-resilience of the critical entities.

NIS2 came into force in 2024

NIS2 Directive

The NIS 1 Directive identified two categories of entities, Essential Service Operators (ESOs) and Digital Service Providers (DSPs), which were subject to two sets of obligations:

- **Security measures** – adoption of security measures proportionate to the risk and aimed at preventing and minimize the impact of security incidents (with more detailed measures in the DSP context).
- **Incident reporting** – notification without undue delay to the competent authorities or to the CSIRTs of incidents having a significant impact on the continuity of the essential services provided (based on the number of users involved, on duration and on geographic take-up).

For its transposition at national level, the NIS1 Directive required of Member States:

- the adoption of a **national strategy** in the cyber-security field with strategic objectives, priorities, adequate policies and regulatory measures at national level;
- **international cooperation and cooperation with ENISA (European Network and Information Security Agency) through the identified mechanisms;**
- **designation of competent national authorities,** contact points and CSIRTs (Computer Security Incident Response Teams), responsible for the security and monitoring of incidents at national level.

The **NIS2** Directive strengthens the obligations already provided for by the NIS1 Directive, overcoming the ESO and DSP classification and **reclassifying the entities subject to regulation in "essential" and "important"**. Among the essential entities we find the "digital infrastructure" (ECN, ECS, cloud, data centre, CDN, etc.).

- **NEW security measures –** maintenance of a "multi-risk" approach in the adoption of adequate and proportionate technical security measures to (i) manage the risks to the security of the network and information systems used by these subjects for their operations or to supply their services and (ii) prevent or minimise the impact of the incidents on the recipients of their services and on other services. The NIS2 provides for a minimum list of the security measures to be implemented.
- **NEW incident reporting –** stronger reporting obligations and notification of "significant incidents" to the competent authorities and to the CSIRT according to a multi-phase scheme with pre-defined times (reduced to 24 hours from the awareness to send an "early warning", followed by the initial notification within 72 hours and a detailed analysis of the incident within a month). Where appropriate, the notification of the significant incidents without undue delay also to the recipients of the services is provided for.

Even the requirements addressed to Member States are stronger, compared both to the provision of supervisory and enforcement measures applicable to essential and important entities (e.g. targeted audits and inspections), and to new information sharing obligations.

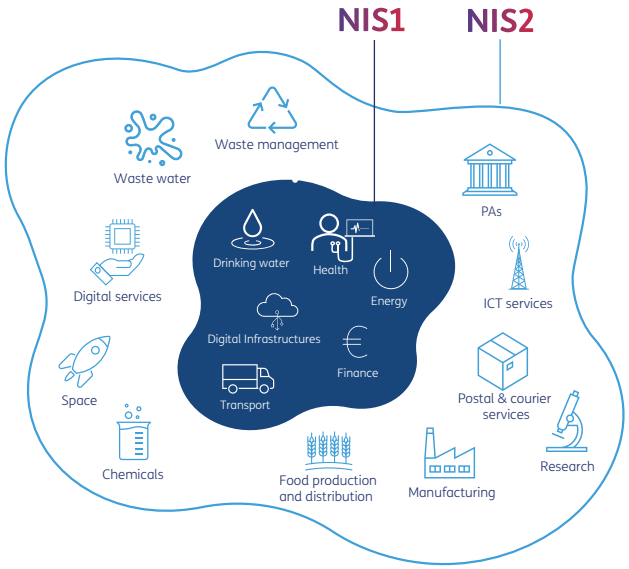
The NIS2 Directive was published in the EU Official Journal in December 2022 and entered into force on 16/01/2023. Member States had 21 months from the entry into force of the Directive to transpose the provisions into their national law (effective date: 18/10/2024) but to date only Italy, Belgium, Croatia, Greece, Lithuania, Romania, Slovakia and Hungary have completed the transposition process.

NIS2:
scope, sectors and scale

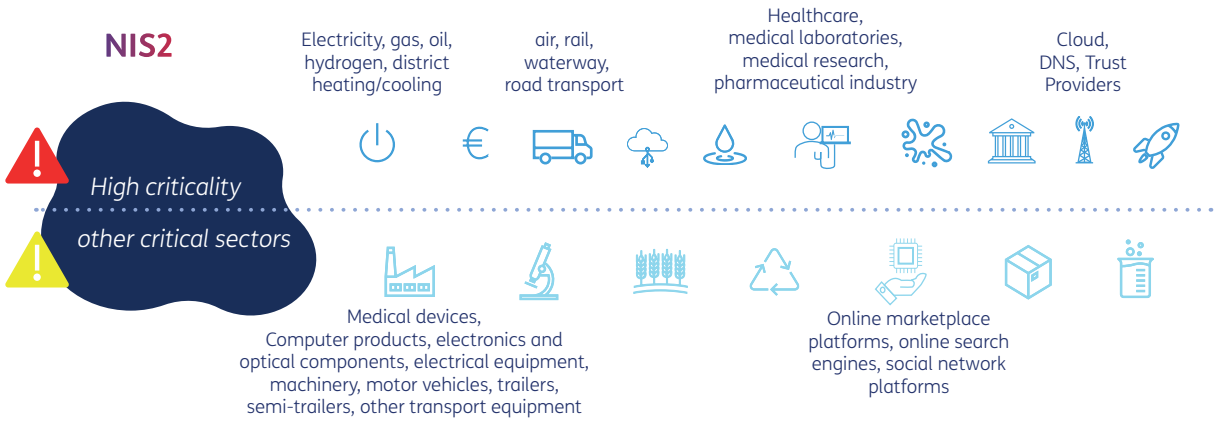
The criteria to define entities subject to regulation under NIS1 have led to differences and inconsistencies in the choices made by the various Member States. To overcome uncertainty and provide greater clarity, a different criterion has been defined, classifying subjects into essential and important entities based on their inclusion in highly critical sectors (compared to critical sectors) and the size of the company.

EXTENDED SCOPE

NIS2 expands the scope of NIS1 by introducing new measures aimed at making the entire European economic system more resilient to external attacks.



CLASSIFICATION OF SUBJECTS AND SECTORS



DIMENSIONAL THRESHOLD

	EMPLOYEES	REVENUES	SECTORS OF **HIGH CRITICALITY**	OTHER **CRITICAL** SECTORS
Large enterprises	250+	M€ 50+	**Essential** entities	**Important** entities
Medium-sized enterprises	50-249	M€ 10-50	**Important** entities	**Important** entities
Small enterprises	< 50	M€ <10	*only if they fall within the sectors defined as critical by NIS2*	
Micro- enterprises	< 10	M€ ≤2		

Activity in 2024:

Cyber Resilience Act (CRA)

The Cyber Resilience Act (CRA), which aims to define cybersecurity requirements for products with digital components, entered into force on 10 December 2024.

This regulation applies to different types of products equipped with hardware components or software systems, from medical instruments to smart toys, which can be violated and used to penetrate connected systems by bypassing security protections. The regulation provides that the products are divided into two different classes depending on the different criticality and risk level. In addition, four specific objectives have been set:

- ensuring that manufacturers improve product safety with digital elements from the design and development phase and throughout the entire life cycle;
- ensuring a consistent cybersecurity framework, facilitating compliance for hardware and software manufacturers;
- improving transparency regarding product security properties with digital elements;
- enabling businesses and consumers to safely use products with digital elements.

The CRA is a horizontal regulation aimed at ensuring a minimum level of security for all hardware and software products circulating in the EU and intertwined with other specific vertical measures (NIS2, systems IoT, etc.).

On 11 Decembre 2024, the European Commission established an expert group to assist and advise the Commission on issues relevant to the implementation of the CRA..

Cyber Security Act (CSA)

The cybersecurity regulation entered into force on 7 January 2024 and specifically:

- strengthens the role of ENISA, the EU agency responsible for cybersecurity;
- provides support to Member States, EU institutions and businesses in key areas, including the implementation of the NIS2 Directive;
- introduces an EU-wide cybersecurity certification framework for ICT products, services and processes.

DORA

The DORA Regulation (Digital Operational Resilience Act) sets the requirements and the technical standards to manage the risks for the financial sector, including third-party ICT service providers among the financial entities.

DORA is the *lex specialis* of the NIS2; therefore, the NIS2 relevant provisions related to the management measures of cybersecurity risks, notification of significant incidents, supervision and enforcement do not apply to the entities subject to DORA.

The provided technical standards entered into force on 17 January 2025.

The Cybersecurity Agencies
A **leading role** in Europe

The actions of the European Union in the cybersecurity field aim to overcome the differences among Member States by creating a single and resilient European cybersecurity system and ensuring a better level of control over the digital borders: This involves addressing some legacies of the past which rely on the institutional structures of individual Member States.

In this context, the European Cybersecurity Agency (ENISA) has a central role based on four cornerstones:

- **Cybersecurity Policy**. ENISA is a crucial skills centre and supports the development of the EU policy on cybersecurity.
- **Operational Cooperation**. It supports the coordination among the different European cybersecurity systems and facilitates a rapid response to large-scale incidents by the CSIRTs network and CyCLONe, the European cyber crisis management structure.
- **Reliable solutions**. ENISA oversees the certification of the equipment safety level, preventing the proliferation of national systems based on different standards.
- **Capacity development.** It enhances flows of information, training and best practices adoption, helping Member States to assess the level of maturity of their own cyber-defence systems.

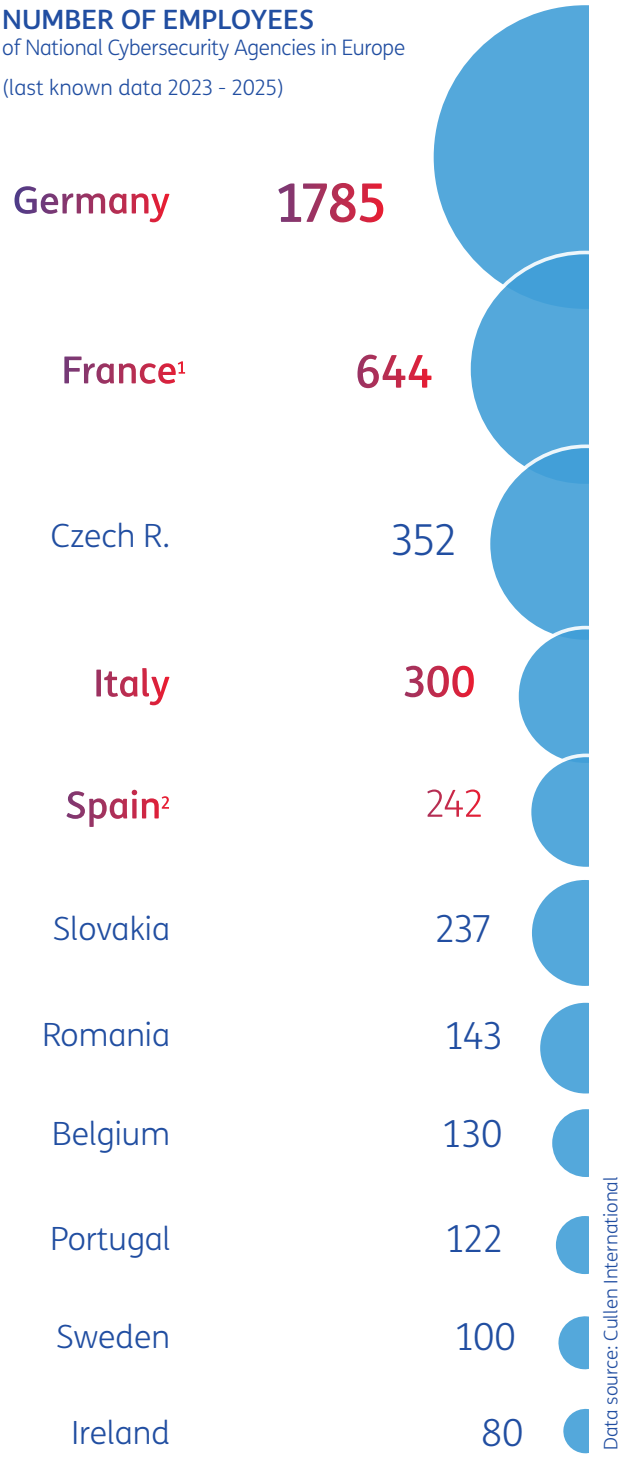
In other terms, ENISA holds a strategic reference, political, technical and operative role for the different national cybersecurity structures, which in turn represent for each country a reference point to ensure a safe and resilient digital environment. The Directives require that these structures be "adequately staffed to ensure ongoing availability" and –operating on the ground to ensure the cybersecurity of the main European Countries –shall host the CSIRT, a technical unit which monitors and responds to incidents aimed at critical infrastructure at national level.

We can appreciate the Agencies' complex and robust network activity by observing the ACN activity framework. In Italy, the National Cybersecurity Agency carries out –among others -the following tasks::

- NIS competent authority and single contact point.
- Authority for the integrity of the telecommunication networks.
- Supervision of the National Cybersecurity Perimeter.
- Qualification of the cloud infrastructure and services for the Public Administration.
- National Assessment and Certification Centre (CVCN).
- Italian CSIRTs
- Cybersecurity Units (NCS)
- Italian National Coordination Centre (NCC-IT) and support of the European Cybersecurity Centre.

EUROPEAN CYBERSECURITY AGENCIES: STAFF

NUMBER OF EMPLOYEES
of National Cybersecurity Agencies in Europe
(last known data 2023 - 2025)



Staff of the National Cybersecurity Agencies

Currently, in Italy, the National Cybersecurity Agency employs approximately 300 people, and its full workforce is expected to reach 800 people, a number in line with France, which in 2022 had just under 800 people working in ANSSI (around 650 FTE in 2024).

In Europe, the country with the most resources is Germany: the BSI (Bundesamt für Sicherheit in der Information Technik) employed approximately 1,700 people at the beginning of 2024. According to press sources, the number of personnel in the Spanish National Cybersecurity Agency is estimated to be between 200 and 250 people.

Budget of the National Cybersecurity Agencies

As to budgets, the situation is less clear because information is not always available, and resources may be allocated across different entities. Based on available data, the German agency BSI has the highest budget, estimated at around 240 million euros, while ANSSI in France has approximately 80 million euros. No updated data is available for Spain (according to 2022 data, however, the budget per employee was the highest among those available). In the Netherlands, the budget has increased due to the consolidation of multiple structures.

1 FTE

2 estimated data

For national security reasons, information on the number of people employed by the UK's National Cyber Security Agency is not public. The latest available data (2019) reported more than 1,000 employees.

FOURTH PART

Emerging technologies

The cybersecurity sector is never stationary. The changes in the geopolitical scenario, the launch of new technological solutions and services, the identification of new flaws and vulnerabilities in the systems, are factors which continuously feed new attack techniques and open unexpected threat fronts.
This is why the scenario must be monitored on a regular basis and the ongoing developments must be kept under control, trying to anticipate as much as possible the opponents' moves, which are often one step ahead of the most advanced defenders from a technological point of view.
The aim of this section is to provide new features emerging from the cybersecurity scenario, both in terms of threats, and of defence, prevention and contrast solutions.

New technical focal points: the **use of AI**

In a global phase of digital transformation, the impact of artificial intelligence (AI) becomes increasingly significant and evident in every sector of society, cybersecurity included. Due to the rapid evolution of its ability to learn, adapt and predict threats, AI has become a sophisticated tool essential for the protection of businesses and governments from the threats deriving from connected technologies: from cyber-attacks to spamming, to information manipulation. At the same time, AI poses new challenges also in terms of attacks due to the growing accessibility and take-up of this tool now widely available to the attackers.

An example of the dual role held by artificial intelligence in the cybersecurity field is represented by generative AI: in response to the barriers in commercial products such as ChatGPT to prevent an improper use of the technology, **antagonistic tools**, such as WormGPT or FraudGPT have been developed, to bypass those barriers and support the cybercriminals in the writing of malicious codes or in malware development.

Generative artificial intelligence is exploited also to launch **phishing campaigns, creating convincing e-mails and misleading messages which are increasingly difficult to detect**, with less use of resources and time than in the past. What is more, the attackers can identify the high value objects in a more efficient way and tailor the attacks aimed at the profiled target though machine learning **algorithms used to analyse social media and other online data**.

AI can potentiate the malware by learning the user's or the system's typical behaviour, allowing attacks or data exfiltration, avoiding the detection by security systems and simulating a normal activity situation.

The AI-based reconnaissance tools enable **network scanning activities looking for vulnerabilities**, choosing automatically the most efficient exploit to carry out the attack. The AI training process enables to identify and select the most valuable information to exfiltrate, further reducing the chances of detection by the security systems.

Ultimately, the attackers exploit the AI to generate audio or video **deepfake** used during phishing or **vishing** (vocal phishing) attacks, impersonating trusted people in a convincing way and conferring higher credibility to social engineering attacks.

In 2019, the voice of the CEO of a British energy sector company was simulated to request an urgent transfer to a supplier based in Hungary and illegally transfer funds.

In March 2022, the cybercriminals hackered an Ukrainian TV channel and uploaded deepfake videos on social networks where president Zelensky asked for the laying down of arms and the surrender to the Russian army.

In May 2022, a deepfake of Elon Musk promising returns up to 30% to the investors of a cryptocurrencies trading platform was uploaded on YouTube.

In May 2023, the Social Proof Security ethical hackers used the vocal clone of a US TV correspondent to induce one of the broadcasting staff members to release sensitive personal information.

New technical focal points:
Quantum computing

Quantum technologies represent another frontier of applied research. The great computational power of quantum computers enables the resolution of complex problems in less time, and this is why these technologies are applied where there is the need to govern the interaction of countless variables (optimisation, planning, simulation etc.). Nowadays it is possible to theorise various developments of the quantum technologies, also in the cybersecurity field.

POTENTIAL THREATS

First, the computational power raises the issue of potential threats. The encryption solutions adopted nowadays are based on keys particularly complex and difficult to break, but not by a quantum computer which can achieve a solution in a short time.

Faced with this possibility, several countries already started to act: the US National Security Memorandum (2022) provides for a migration to quantum-resistant cryptography by 2035. In Europe, the European Commission launched the Euro-QCI (Quantum Communications Infrastructure) project, based on the distribution of quantum cryptography keys (QKD, Quantum Key Distribution). This infrastructure should be used mainly to exchange information between government agencies and authorities of the Member States and the EU.

The QKD, together with Post-Quantum Cryptography (PQC), is the main approach adopted at global lever for the transition to quantum-resilient cryptographic systems.

The PQC provides for the design of particularly complex classic cryptographic schemes deemed resistant also to quantum computers. The QKD is a physical level method based on quantum mechanics, which provides unconditional security, i.e. security that is independent of the relevant computational model.

DEFENCE OPPORTUNITIES

At the same time, the computational power represents an opportunity of defence: quantum physics enables to implement photon-based encryption keys, such as the above-mentioned QKD, consisting of a synchronous system to exchange symmetric keys to protect the exchange of highly sensitive data (ex. healthcare data, financial data etc.). The potential violation of the key is detected immediately by those exchanging the encrypted data, enabling them to stop the exchange and generate a new key.

Another interesting evolution is the Quantum Number Random Generation (QRNG) an application to generate random numbers exploiting the physical properties of the natural phenomena generating entropy to overcome the limit of the current algorithms used by traditional computers where the generation occurs through a deterministic numerical trigger.

A further evolution to be noted is the one of the microprocessors for cybersecurity applications based on quantum technologies. In this perspective, Telsy developed a Secure Microchip, a programmable and secure-by-design micro-platform using PQC algorithms to ensure a defence also against quantum opponents. For its innovation, the Secure Microchip was designated among the best technological innovations by the GSMA, the global TLC operators' association.

Conclusions

by Ivano Gabrielli

Director of the Postal and Communications Police Service

2024 can be considered, in all respects, a "zero" year for cybersecurity in our country. In fact, we have witnessed a phase of profound transformation, in which institutional focus, regulatory evolution, the maturation of operational structures and the growing awareness of economic actors have defined a new perimeter for national digital security.

The cyber threat, which has significantly grown, is no longer limited to targeting critical and sensitive infrastructures. It is increasingly manifesting as a systemic phenomenon, transversal and interconnected with global geopolitical dynamics. Continuous and targeted attacks on the public administration and the country's strategic sectors are detected, but the impact is particularly significant for small and medium-sized enterprises. SMEs, representing 63% of the Italian economy, remain the weak link in the system, often lacking the economic resources and technical skills necessary to adopt adequate cybersecurity measures. This makes them prime targets for organised crime and hostile groups, which exploit these vulnerabilities to conduct increasingly sophisticated attacks.

Faced with this scenario, the need for a paradigm shift emerges. Cybersecurity must be structurally integrated into the companies' organisational and production models, with the same logic with which the digitalisation process was addressed in the past or the physical security of company assets was guaranteed. Secure design of systems and processes, according to the principle of cybersecurity by design, must become the norm. Businesses, especially SMEs, are to be guided towards sustainable solutions such as purchasing remote security services or joining sector consortium structures capable of offering shared monitoring and incident response services through common SOCs and CSIRT. This approach represents a concrete response to the need to distribute costs and skills within a fragmented but vital production ecosystem.

It must be said that Italy, whose economy is strongly based on the manufacturing sector, has characteristics similar to those of other European countries such as France and Germany. The data show substantial consistency with the international picture, but this cannot and must not represent an element of reassurance. Along with the numerical growth of attacks, the high complexity of digital offensives is worrying, often orchestrated by structured criminal organisations capable of accessing a global market of criminal technology. The threat, therefore, is both more frequent and complex and difficult to address with conventional tools.

From an operational point of view, there has been a significant maturation of the processes adopted both by law enforcement structures and institutions, with the establishment of faster and more effective mechanisms to address cyber threats, in order to make the national system more consistent, resilient and reactive. It is precisely in this context that the strengthening of the territorial structures of the Postal Police takes place: these serve as a real backbone for the prevention and fight against cyber-crimes, supporting the District Attorney's Offices and allowing investigative actions to be integrated with a continuous and qualified technical presence.

At the regulatory level, a decisive role was played by the implementation of the NIS2 directive and the approval of Law no. 90, dated 28 June 2024. These tools have redefined the relationships among the main entities involved in cybersecurity governance, in particular between the National Cybersecurity Agency, the judicial authority and the Law Enforcement structures. The tools have introduced elements of clarity, shared responsibilities and greater interinstitutional cooperation. The result is a more structured regulatory environment, capable of supporting an organic response to digital threats.

Significant progress has also been made in the field of investigative tools, with the adoption of increasingly advanced technologies essential for dealing with sophisticated and transnational attacks. This modernisation has enabled a qualitative leap in the response capacity of law enforcement, enhancing the ability to promptly identifying threats, reconstructing their origin and intervene in a targeted manner, even in a context where the boundaries between criminal and strategic threats are increasingly blurred.

The data clearly show how Italy must prepare to live with a constantly high level of risk in the coming years. This is not a contingency, but a structural condition that requires the establishment of a permanent and inter-institutional presence, capable of guaranteeing a continuous, updated and coordinated response capacity. In this way, it will be essential to strengthen the public-private partnership, establishing it as the pillar of a distributed, resilient and sustainable cybersecurity system.

Therefore, 2024 was a turning point both for the consolidation of existing capabilities and for the start of a new strategic phase for national digital security. Institutions have made a significant effort to build an operational capacity capable of addressing the complex threats that characterise today's cyberspace, threats that simultaneously affect individual freedoms, essential public services and primary economic assets.

The Italian regulatory framework is cutting-edge in the European context. However, an element that cannot and must not be underestimated is the need to promote strong and coordinated investment in skills training, with the introduction of innovative training models. It is necessary for the State undertake efforts to create a new generation of cybersecurity experts, trained to be immediately operational in institutional roles and subsequently able to contribute, also in the private sector, to the strengthening of the national cyber presence. From this perspective, the opportunity for a pact between institutions and the economic world emerges, capable of supporting a training cycle that is useful today for the public, and tomorrow for the private, in the construction of a truly participatory and efficient cybersecurity ecosystem.

We would like to thank **Hon. Alessandro Colucci**, Secretary of the Presidency of the Chamber of Deputies and President of the “Parliamentary Intergroup for Information and Technological Security”, for encouraging the development of this report and for the interest shown in spreading cyber awareness at a national level..

Our thanks to ACLED (Armed Conflict Location & Event Data) and Cullen International for the data provided.

The cover image was generated by AI.

CYBER SECURITY FOUNDATION

TIM

Cyber Security Report

DDoS and Ransomware threat analysis

June 2025

www.gruppotim.it

www.cybersecurityfoundation.it