
CYBEROO
CYBEROO
OBSERVATORY
2025
2025 EDITION

Via Brigata Reggio 37, 42124, Reggio Emilia, Italy
e-mail info@cyberoo.com
www.cyberoo.com

CONTENTS

“Giving an outlook into the long-term future, the increased dependencies and the development of new technologies, such as quantum computing and AI, add complexity to the threat landscape and introduce new risks for which further preparedness is needed.”

INTRODUCTION

If there is one recurring factor in the cyberspace in which we operate, it is the increase in **cyber attacks**. It is expected that business losses caused by cyber attacks will grow significantly, reaching **$10.5 trillion** by 2025. This staggering increase can be attributed to the exponential growth in attacks, which in 2024 reached a **monthly average of 273**.

It is not just the quantity of attacks, but also the increasing sophistication, with 81% of cases classified as critical or high severity. To defend yourself, you must not only identify your vulnerabilities but also develop a deep understanding of the **latest techniques** used by cybercriminals. In this document, we present the results of the **CYBEROO Observatory**, which analyzes the trends, emerging threats, types of attacks, the most common vulnerabilities detected, the main threat actors, and the most effective strategies to defend yourself in 2025.

INTRODUCTION

CYBER ATTACKS: IMPACTS AND COSTS

Cyber attacks pose a constant threat to organizations. Our Incident Response team, which provides on-site support in the event of an incident, has seen many in recent years: from companies that have experienced IT system **malfunctions**, website manipulations, operational disruptions, and **loss of productivity** to those forced to shut down or lay off their entire staff. In other cases, there has been the **disclosure of sensitive documents** such as patents or the unauthorized opening of bank accounts in the names of employees.
Cybercriminals are able to compromise **the entire security of your data**, with devastating financial and operational impacts, including:

- The **breach of confidential data**, theft of trade secrets, and unauthorized disclosure.
- The **malfunction of IT systems** caused by website manipulations or attacks, with operational disruptions and loss of productivity.
- The **payment of hefty ransoms**, as well as the loss of reputation, customer trust, and revenue.

In this context, companies must adopt **preventive cybersecurity measures** to protect their digital assets and ensure business continuity.

INTRODUCTION

CYBER ATTACKS: THE CONSEQUENCES

- Business disruption
- Legal expenses and fines
- Damage containment costs
- Reputational damage
- Civil liability for senior corporate executives
- Privacy violation
- Intellectual property theft
- Loss of competitiveness
- Loss of profitability
- Data breach and disclosure
- Ransom and data extortion
- Loss of loyal customers

LEGAL FRAMEWORK IN EUROPE

The time for avoiding responsibility is over—every board of directors must now be accountable. If 10 years ago investing in cybersecurity appeared to be a foresight of the most forward-thinking minds, now it is a **regulatory requirement** that affects all sectors and businesses, from microenterprises to larger companies.

On the one hand, the **NIS2 Directive** requires companies to strengthen their cyber resilience and enhance supply chain security, while the **DORA Directive** strengthens resilience and security by establishing a framework for ICT risk management in the financial sector. In addition, the **AI Act** adopts a risk-based approach to ensure a baseline, horizontal level of protection, where security requirements and measures are proportionate to the risks posed by different AI systems. It classifies these systems based on their potential impact on **fundamental rights, health, and safety**. Considering this regulatory framework, companies must invest in specialist skills, adopt **innovative technologies**, and review their **organizational models** to ensure compliance with the new regulations and, above all, to protect their business from increasingly sophisticated cyber threats.

“Cybersecurity leaders need to balance comprehensiveness with agility, combining cyber risk management activities, capabilities, people and technology.”

Gartner®

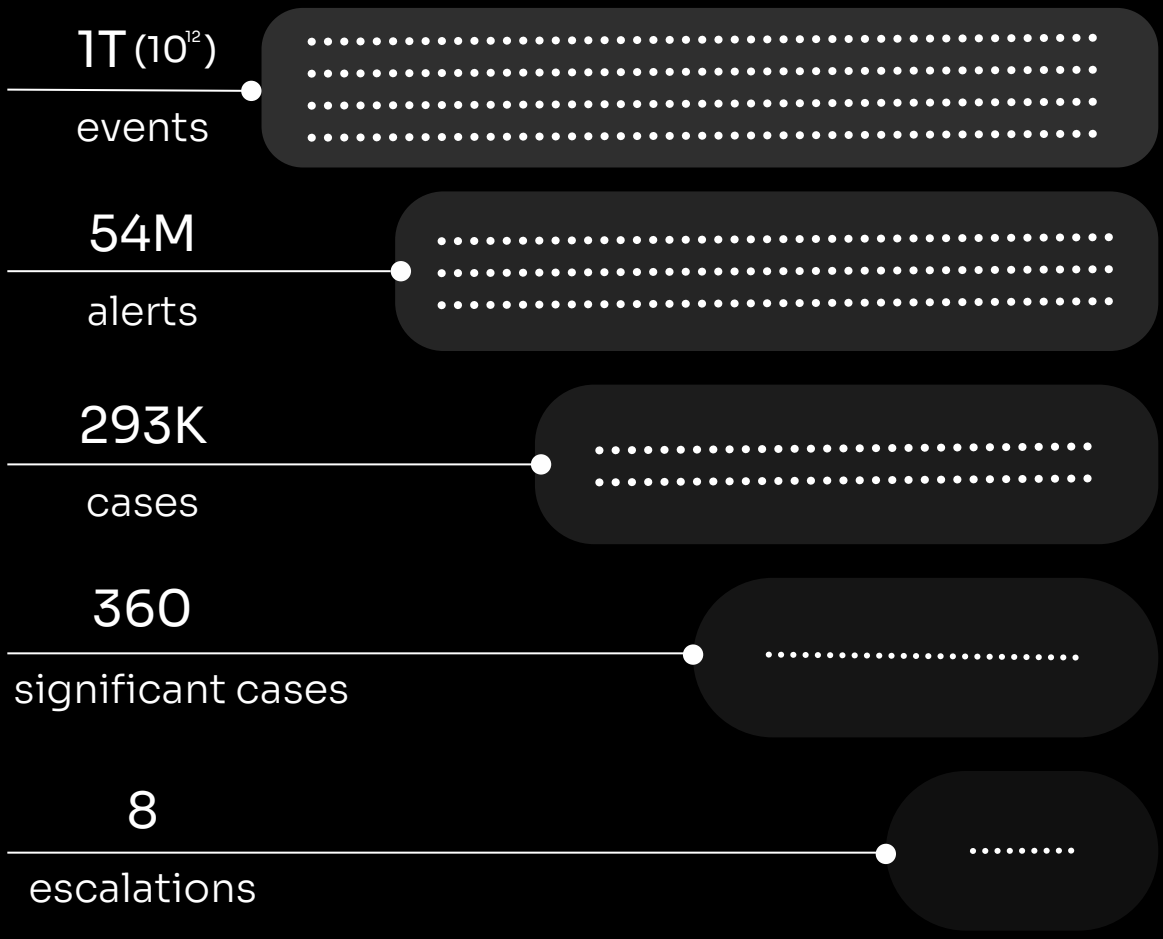
CYBEROO

CYBEROO **OBSERVATORY** 2025

RESEARCH METHODOLOGY

To present the **CYBEROO Observatory** data, our I-SOC team adopted a rigorous methodological approach. The research began with the **classification of events** into alerts, cases, significant cases, and escalations, providing a clear view of operational priorities. Calculation of the Mean Time To Repair (MTTR) incidents was critical to assessing the effectiveness of responses and identifying areas for improvement. We conducted an in-depth analysis of the trends in 2024, identifying the **most common types of attacks** and the **most exploited vulnerabilities**. We quantified the total number of adversaries and identified the key **threat actors**, updating the threat framework. Looking ahead to 2025, we examined **emerging attack vectors** and made **strategic recommendations** for addressing those threats, based on empirical data and predictive analytics. To enrich the analytical context, additional data, such as information on past incidents and the behavioral patterns of attackers, was integrated. This holistic approach has created a solid foundation on which to tackle **future challenges** in the cybersecurity landscape. It should be noted that in order to protect the privacy of the affected companies, we have anonymized all the cases mentioned.

MANAGED EVENTS 2024



The figure shows the distribution of events managed by the CYBEROO I-SOC team in 2024, classified into four categories: **alerts**, **cases**, **significant cases**, and **escalations**.
Alerts are initial notifications of potential security anomalies. Cases require further investigation and become significant if they have a major impact on security. Escalations require action by the Incident Response Team.

MEAN TIME TO REPAIR A NON-INCIDENT EVENT

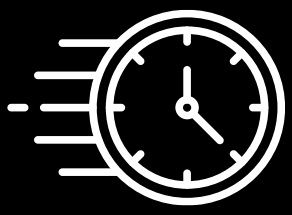
2 HOURS 22 MINUTES

The Mean Time To Repair (MTTR) is a metric that quantifies the **average time it takes** to identify, analyze, resolve, and close an event after its detection. It includes all **operational phases**: from diagnosis to final resolution. In 2024, the CYBEROO I-SOC team resolved events that did not turn into an incident in an average time of 2 hours 22 minutes. Non-incident events are suspicious activities that have not yet caused damage to the information system. Promptly detecting and blocking them can help prevent **future escalations**. Below is the mean time to repair an incident for companies that have contacted us in on-demand mode.

MEAN TIME TO REPAIR AN INCIDENT

5.4 days

CYBEROO
MEAN



22 days

WORLD
MEAN

TRENDS OBSERVED IN 2024

TRENDS OBSERVED IN 2024

In 2024, the CYBEROO Observatory highlighted **four significant trends**:

1. INCREASE IN PERSONAL DATA BREACHES

Attempts to attack corporate databases protected by CYBEROO solutions increased by 25% compared to 2023, particularly in relation to sectors such as healthcare and financial services. The findings of the CYBEROO Observatory are consistent with those of the authorities, which in 2024 were also involved in managing new cases of digital chaos caused by cyber attacks on private and public entities, including government bodies, and banking and health institutions, following the high-profile cyber attack on a local health authority in December 2023.

2. INCREASE IN RANSOMWARE CAMPAIGNS

An average increase of 30% in targeted cyber attacks demanding ransoms was observed. Multiple European SMEs and institutions have been targeted by ransomware attacks, echoing the trends reported in national media. One such example involved a football team in Northern Italy that suffered the theft of sensitive data including documents, personal information, contracts, bank details, and a ransom request.

218 FILES OF CREDENTIALS

BELONGING TO CITIZENS FOUND FOR SALE ON THE DARK WEB.

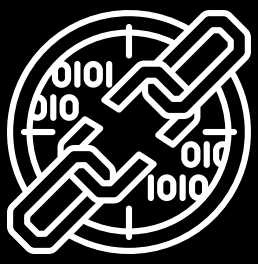
TRENDS OBSERVED IN 2024

3. USE OF GEN-AI BY ATTACKERS

We have seen an increase in the use of AI to create more convincing phishing e-mails and to bypass defenses based on traditional algorithms. A phishing campaign conducted against a well-known bank used AI to fake realistic internal communications, deceiving over 200 employees. Attackers also used AI to create fake e-mails coming from Government agencies, targeting companies in the public and private sectors. One example was an attack involving a large public transport company, which was quickly identified and neutralized.

4. CONSOLIDATION OF SUPPLY CHAIN ATTACKS

The CYBEROO Observatory identified an unprecedented increase in adversaries who have exploited vulnerabilities in IT service providers to deceive employees and cause large-scale damage. In 2024, an attack on a management software provider that compromised over 150 of its business customers made the headlines. Another significant case involved an IT service provider in the energy sector, where an attack on the provider caused operational disruptions for several industrial customers.



1,473 UNIQUE CVEs IDENTIFIED WITHIN SUPPLIER SYSTEMS

OF WHICH 177 WITH CVSS (V3) CRITICAL LEVEL
& 456 WITH CVSS (V3) HIGH LEVEL

MOST COMMON TYPES OF ATTACKS 2024

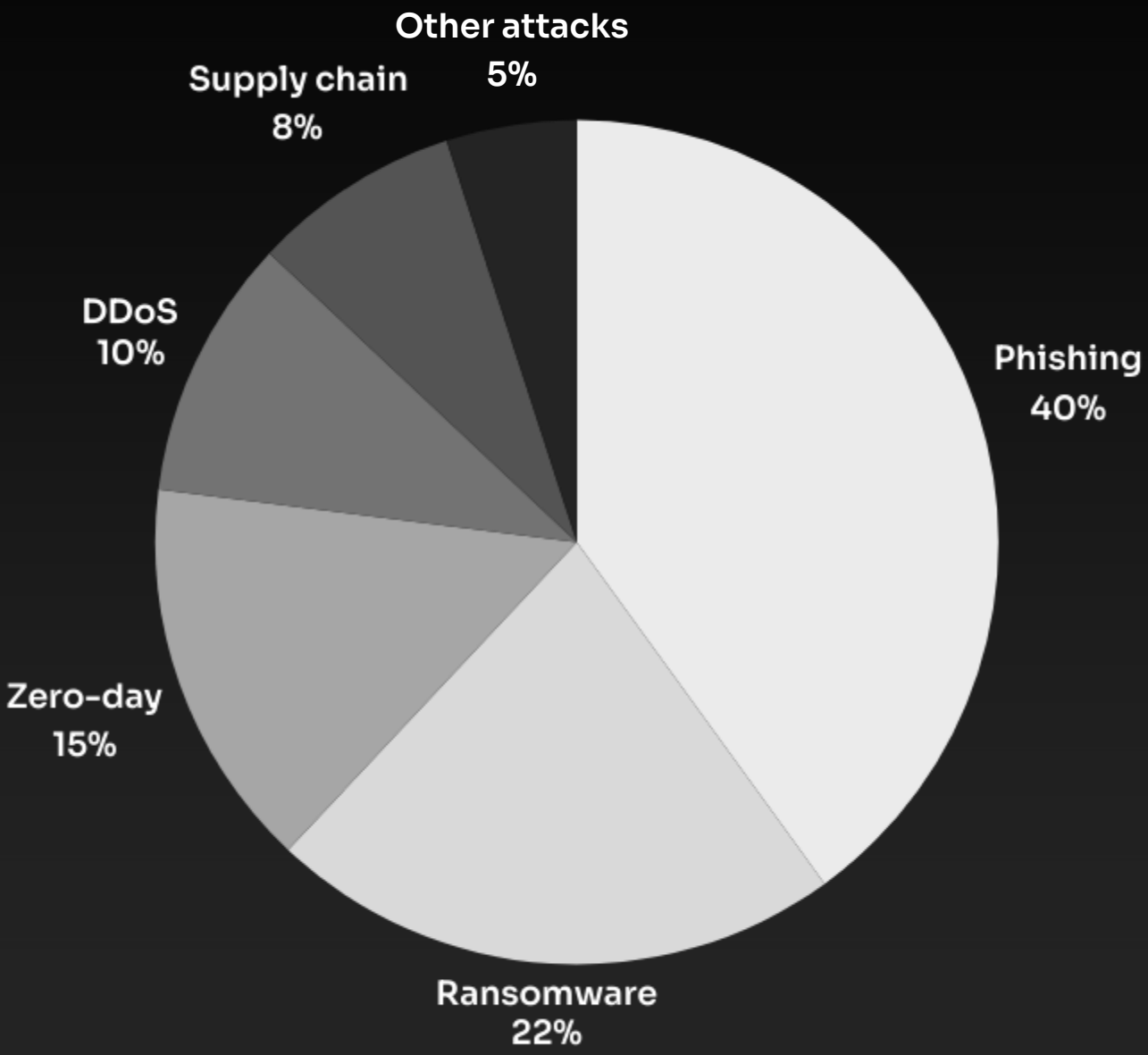
“We are surrounded by invisible threats—sometimes, all it takes is the right visualization tool to reveal them. The real danger is tackling them blindfolded.”

Matteo Ghiotto
Chief Technology Officer

CYBEROO

MOST COMMON TYPES OF ATTACKS 2024

The CYBEROO Observatory identified the following types of attacks as the most common in 2024.



MOST COMMON TYPES OF ATTACKS 2024

Let’s look at them in detail.

PHISHING AND SPEAR-PHISHING – 40%

These are worrying numbers both from a quantitative point of view, in terms of the growth of attacks, and from a qualitative perspective, given the sophistication of the techniques used; this not only includes the use of artificial intelligence but also the increasing usage of malicious domains, videoconferencing platforms or file sharing tools. It remains one of the main cyber attack vectors and one of the initial access techniques most exploited by attackers.

RANSOMWARE – 22%

In real terms, this is one of the most prevalent threats in the European cyber landscape, as we saw previously. Spread mainly with the help of phishing or spear-phishing generated with artificial intelligence but also through the exploitation of domains, vulnerabilities or compromised credentials, it plays its trump card—the sale of stolen data on the dark web—to extort money from companies in exchange for the supposed deletion of stolen sensitive information.

29,191 SUSPICIOUS DOMAINS DETECTED

AMONG THESE, 900 MALICIOUS CASES PROMPTED US TO LAUNCH TAKEDOWN MEASURES.

MOST COMMON TYPES OF ATTACKS 2024

ZERO-DAY EXPLOITS – 15%

The exploitation of zero-day vulnerabilities, in addition to the delayed installation of patches or updates by companies, makes this type of attack a very common and ever-present vector.

DDoS – 10%

According to its own estimate, Cloudflare blocked approximately 21 million DDoS attacks, a type of attack that is statistically on the rise, registering an increase of 53% compared to 2023. Botnets of IoT devices exposed on the internet and compromised are still heavily exploited and involved in such attacks.

SUPPLY CHAIN ATTACKS – 8%

A very prevalent phenomenon that needs addressing, these attacks directly involve organizations by leveraging the relationships and trust they have with software manufacturers, IT providers, distributors, and even external contractors.

OTHER ATTACKS – 5%

We have identified other types of attacks, including insider attacks, advanced social engineering, and cryptojacking.

MOST COMMON VULNERABILITIES FOUND 2024

MOST COMMON VULNERABILITIES FOUND IN 2024

The most exploited vulnerabilities in 2024 included those relating to operating systems, MFA, and the cloud.

CVE-2023-27997

A heap-based buffer overflow vulnerability affecting some versions of FortiOS and Fortiproxy SSL-VPN. This vulnerability, if successfully exploited, allowed remote attackers to execute code or commands via specifically crafted requests.

CVE-2023-4966

Also known as Citrix Bleed, this is a buffer overflow vulnerability that affects and has affected some versions of Netscaler ADC devices when configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA virtual server. This vulnerability, if successfully exploited, allows unauthenticated remote attackers to access sensitive information such as, in this case, session tokens.

MOST COMMON VULNERABILITIES FOUND IN 2024

CVE-2024-6387

Also known as regreSSHion, this is a vulnerability that affected OpenSSH servers (SSHD) allowing, if successfully exploited, remote code execution with root privileges. This vulnerability arises from a race condition within the SSHD process of the OpenSSH servers that allows an attacker to execute code with root privileges.

CVE-2024-53704

Authentication bypass vulnerability detected in some outdated versions of SonicOS used in SonicWall firewalls. This vulnerability affects the SSL-VPN authentication portal that is normally exposed on the internet. If successfully exploited, an unauthenticated remote attacker can bypass multi-factor authentication and gain unauthorized access a valid SSL-VPN session.

CVE-2024-8963

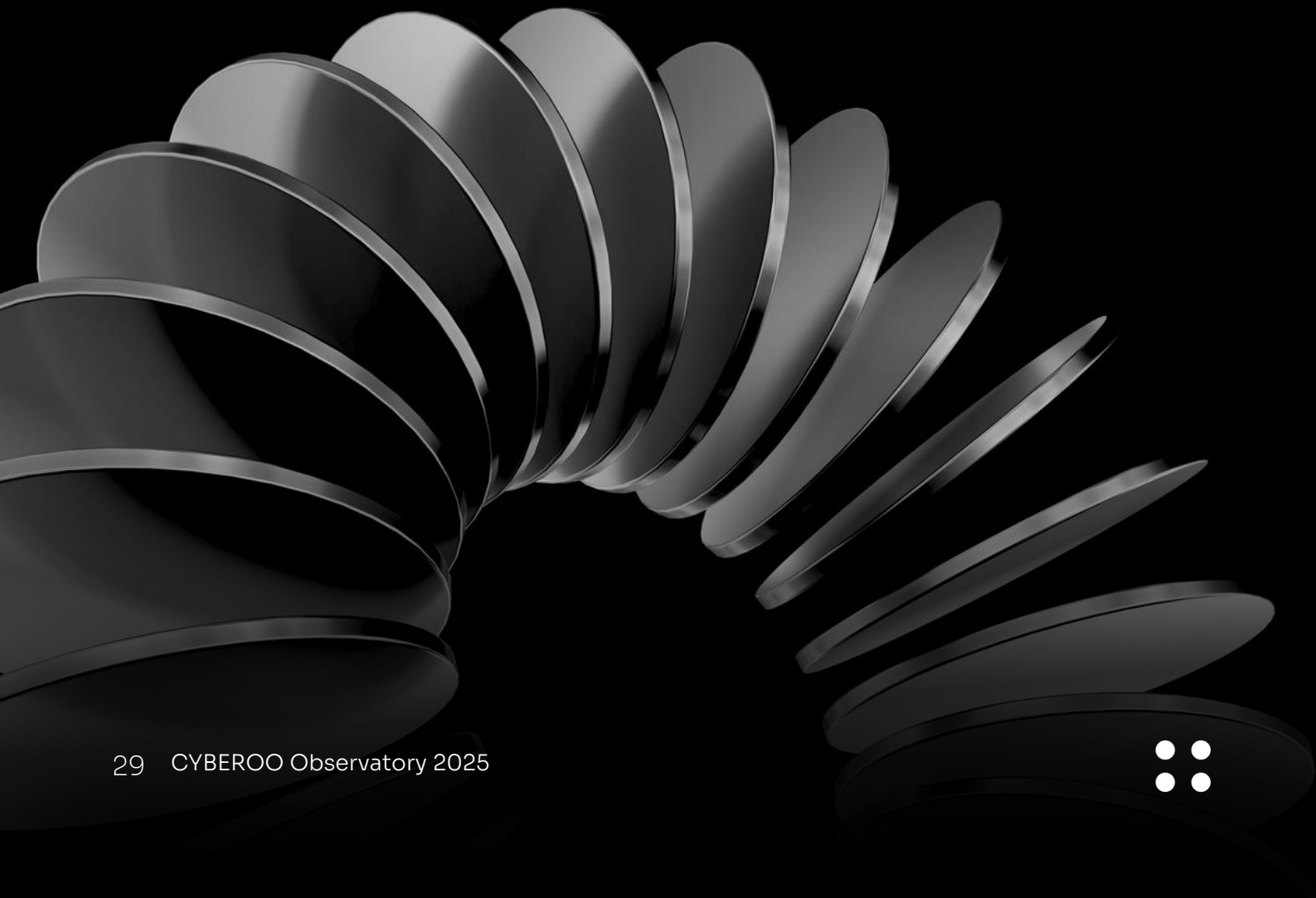
This CVE relates to a critical path traversal vulnerability in the Ivanti Cloud Services Appliance product that allows unauthenticated attackers to remotely execute code, giving them access to restricted functionalities.

MOST COMMON VULNERABILITIES FOUND IN 2024

CVE-2024-11639

Authentication bypass vulnerability detected in some versions of the Ivanti Cloud Services Appliance product. This vulnerability, if successfully exploited, allows unauthenticated attackers to obtain administrative privileges.

REAL-TIME UPDATES



MAIN THREAT ACTORS IN 2024

350 THREAT ACTORS IDENTIFIED

MAIN THREAT ACTORS

Threat actors are constantly evolving. Here are the most active ones we observed in 2024:

INTERLOCK

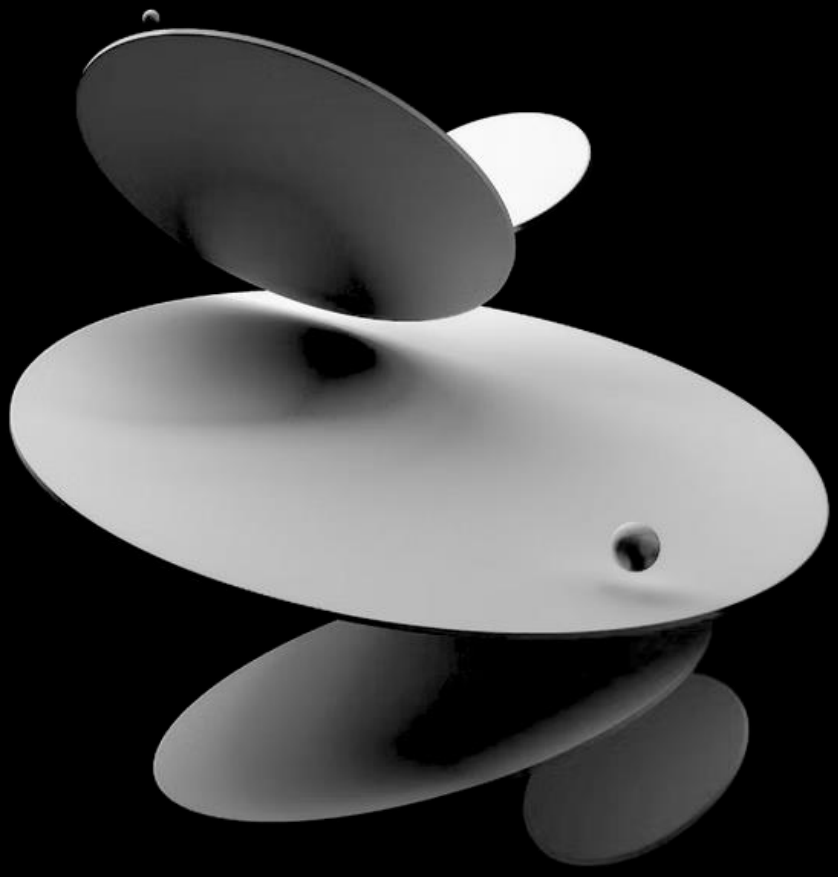
With its name deriving from **International Locker**, this is a 2024 cybercriminal group that operates via **Ransomware** and **double extortion**. It targets organizations in different sectors and some manufacturing companies in Europe, indicating that it does not have a specific target but is simply driven by opportunities. The group claims to be partly motivated by the desire to make companies aware of their poor cybersecurity posture. Once a victim is compromised, this is published on the group's data leak site known as the "Worldwide Secrets Blog" to increase the pressure on the company involved and push them to pay a ransom.

The initial compromise in some attacks occurs through fake Google Chrome updates downloaded from legitimate sites that have previously been compromised. In reality, the Chrome update is a remote access tool that begins to retrieve information about the victim host and establishes an initial connection with a C2 server. The attack begins with an initial reconnaissance phase, followed by persistence and lateral movement, ultimately leading to ransomware execution and a ransom demand.

MAIN THREAT ACTORS

BLACKBASTA

A ransomware group that operates as a **RaaS** (Ransomware as a Service) platform and employs double extortion methods, demanding a ransom to decrypt the data and prevent its disclosure. This group uses a combination of phishing, botnets, and social engineering to gain initial access to the victim's infrastructure. Subsequently, using evasion techniques, it carries out internal reconnaissance and lateral movement aimed at finding critical assets and data before executing the ransomware and encrypting the infrastructure.



MAIN THREAT ACTORS

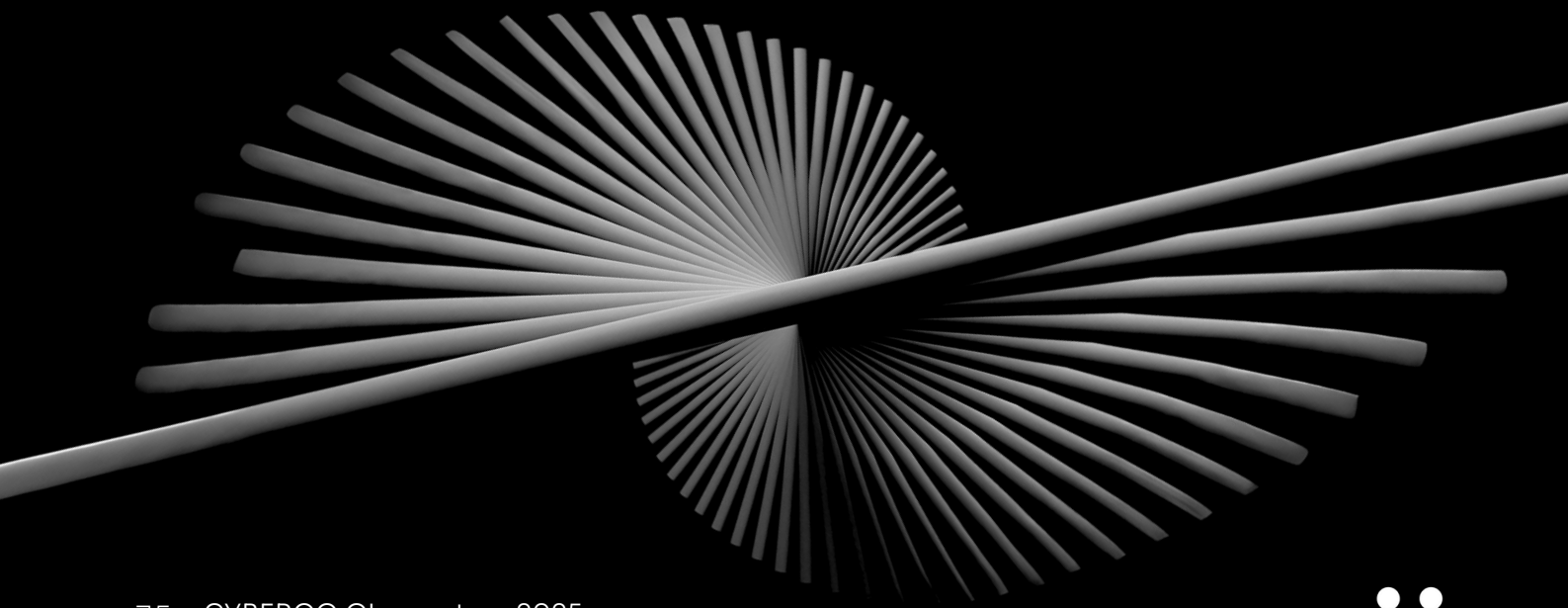
8BASE

A ransomware group that employs **double extortion methods**, demanding a ransom to decrypt the data and prevent its disclosure. 8Base says it only targets organizations that have been careless and have neglected the privacy and importance of their employees' and customers' data. The initial access phase is typically achieved through phishing e-mails. It was also observed that the malware was downloaded during this initial phase via proxy systems or remote access tools. It is equipped with evasion systems capable of disabling Windows Defender and using allowlists for malware paths through Windows Management Instrumentation Command-Line (WMIC) functionality. This group also uses Rclone for the exfiltration phase.

MAIN THREAT ACTORS

RANSOMHUB

A ransomware group operating as a **RaaS** (Ransomware as a Service) platform. This collective appears to follow certain rules such as not attacking non-profit organizations and not targeting victims who have already paid. The “success” of this RaaS would seem to be partly attributable to the group’s recruitment of affiliates on RAMP (Russian Anonymous Marketplace), a predominantly Russian Dark Web forum. After initial access through spear-phishing or compromised VPN credentials, the group performs several actions including initial recognition, privilege escalation, persistence and lateral movement until the execution of the malware. Like other collectives, Ransomhub also appears to use Rclone for the exfiltration phase.



MAIN THREAT ACTORS

AKIRA

A ransomware group operating as a **RaaS** (Ransomware as a Service) platform. Around 300 attacks were estimated for this group in 2024 alone, involving victims in various sectors such as manufacturing, real estate, healthcare, etc. Akira is presumed to be of Russian origin, as an analysis of the ransomware code suggests that it would be deactivated if the compromised host uses a Russian keyboard. Initial access usually exploits weaknesses in firewalls, VPNs, or cloud services. Subsequently, through tools such as IP scanner or Adfind, it carries out a reconnaissance phase for critical services, executes the malware, guarantees persistence, and manages to exfiltrate data through tools such as WinSCP and Rclone.

MAIN THREAT ACTORS

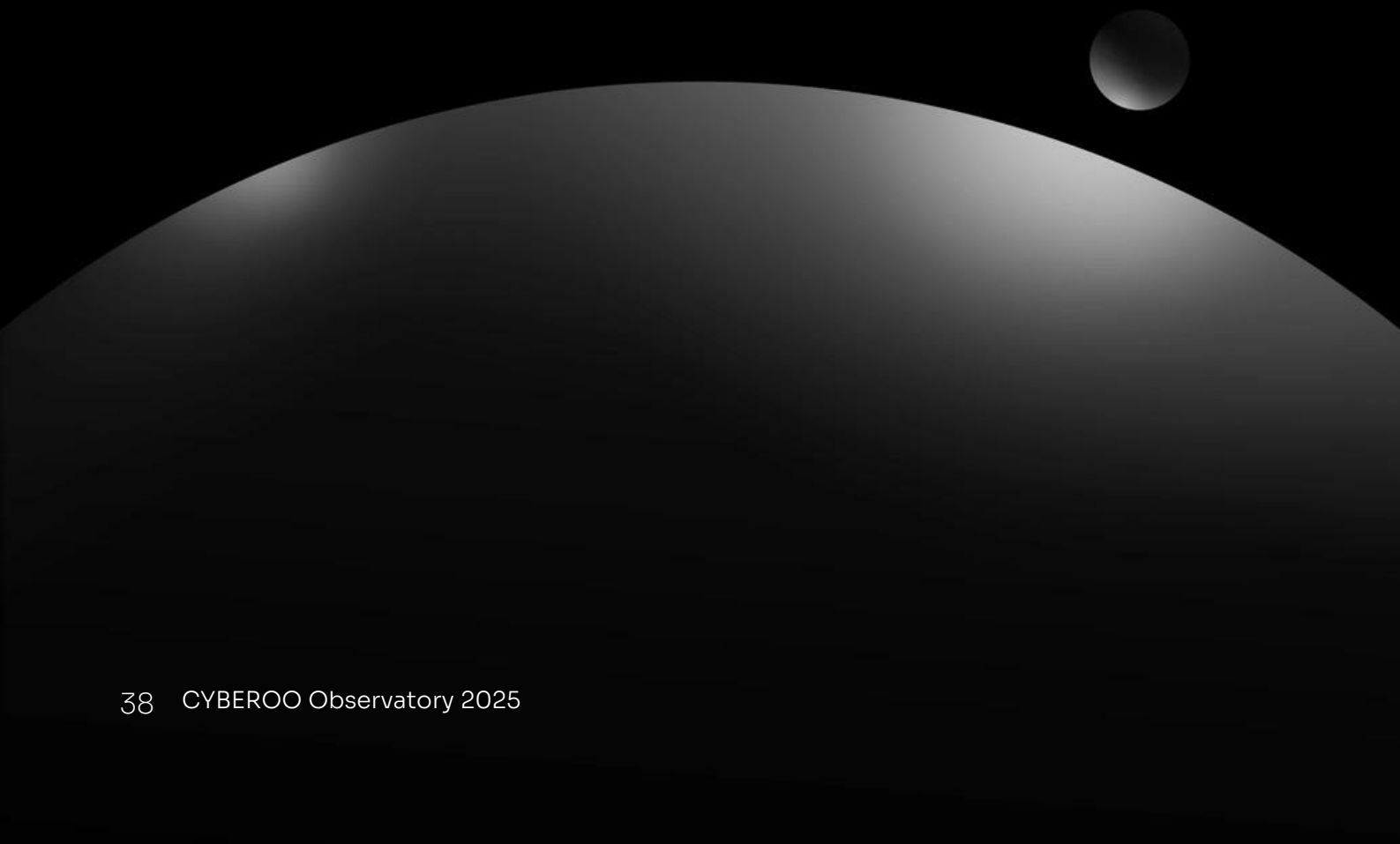
NONAME057(16)

A collective of **pro-Russian hacktivists**. This group is known for Distributed Denial of Service attacks that target government agencies, the media, and private companies in Ukraine, the United States, and Europe with the sole aim of silencing anti-Russia organizations. All participants in Noname057(16) initiatives support the “DDoSia Project”, named after the Dosia bot (toolkit), made available on a dedicated Telegram channel.

HACK_N3T

A Russian hacker collective particularly active in cyber attacks in the context of geopolitical conflicts. It was one of the most active groups, claiming multiple attacks, especially in the first half of 2024. hack_n3t operates through denial-of-service attacks.

INQUIRY: ATTACKS RECORDED BY HONEYPOTS



INQUIRY: ATTACKS RECORDED BY HONEYPOTS

Vasily Kononov, Threat Intelligence Lead at CYBEROO, carried out a study to better understand the current trends of cyber attacks by configuring various **honeypots**—decoy systems for cyber attacks—on a dedicated mini PC, with Ubuntu Server, located in the DMZ zone of a suitably configured network. This simple setup, which is also often used by companies for research purposes, made it possible to **monitor attacks in real time** and analyze the methods, exploited vulnerabilities, and malware families involved. The purpose of this inquiry is not to provide absolute results, but to offer an overview of current trends, which is useful for developing more effective defense strategies. The key findings are outlined below.

INQUIRY: ATTACKS RECORDED BY HONEYPOTS

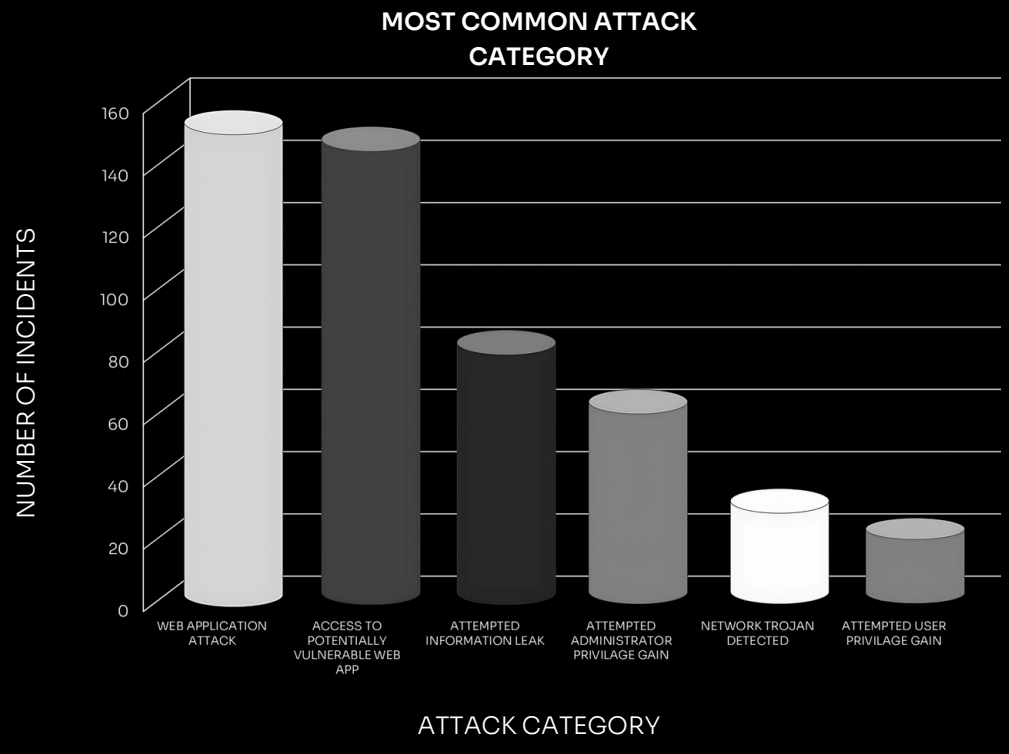
OVERALL ATTACK ACTIVITY

During the 10 days of data collection, 2 million attacks were recorded by different honeypots.

ATTACK METHODS

The “Attempted Administrator Privilege Gain” category dominates with 527 incidents.
The most common techniques identified are:

- Exploiting vulnerabilities to **bypass authentication**
- Attacks on vulnerable **web applications** (e.g., Log4Shell).

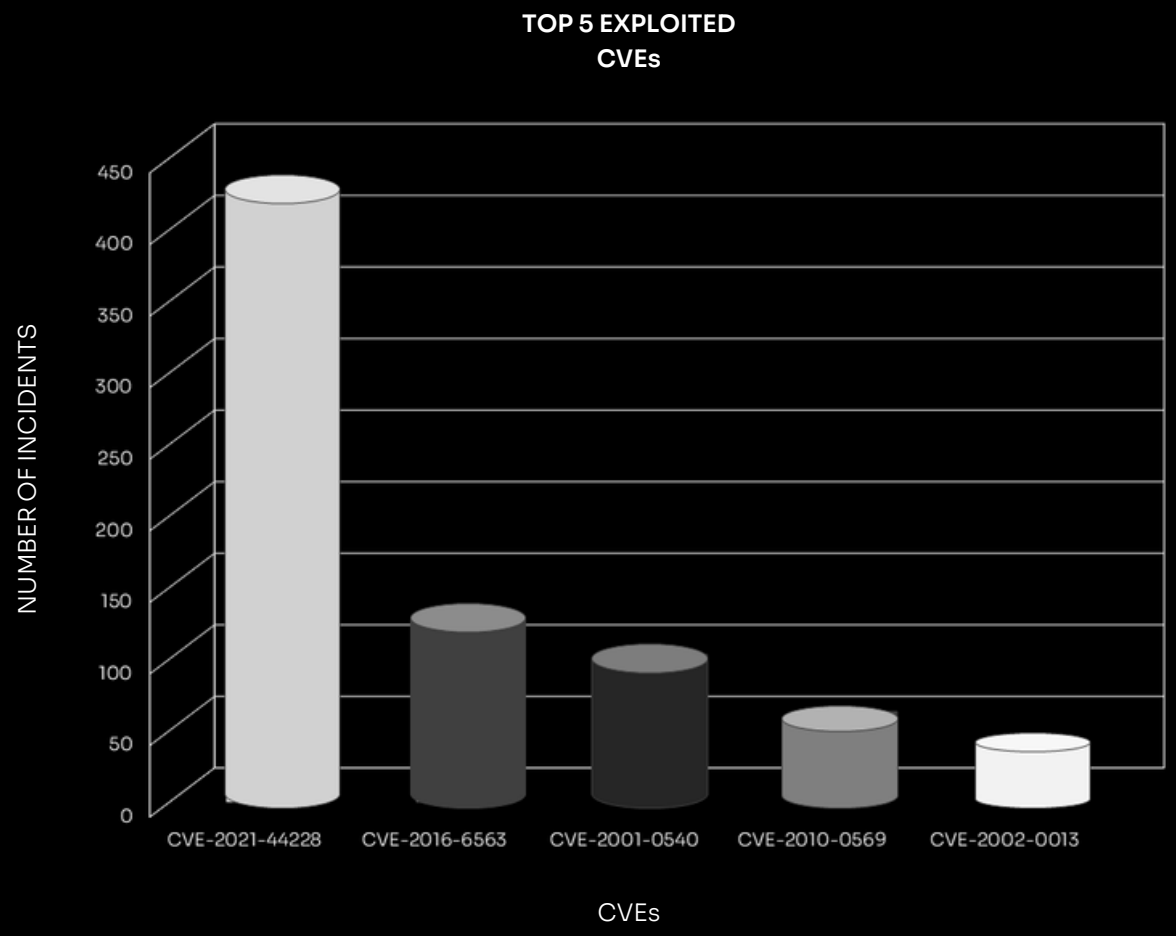


INQUIRY: ATTACKS RECORDED BY HONEYPOTS

VULNERABILITIES EXPLOITED

TOP 5 CVEs:

1. CVE-2021-44228 (Log4Shell)
2. CVE-2016-6563
3. CVE-2001-0540
4. CVE-2010-0569
5. CVE-2002-0013



INQUIRY: ATTACKS RECORDED BY HONEYPOTS

MOST TARGETED PORTS

The most frequently attacked ports are:

- 22 (SSH)
- 445 (SMB)
- 80 (HTTP)

MOST AFFECTED PRODUCTS (ALERT.METADATA.AFFECTED_PRODUCT)

- HTTP Server - 35% of attacks
- IoT devices (routers, cameras)
- Outdated business applications.

MAIN MALWARE FAMILIES (ALERT.METADATA.MALWARE_FAMILY)

- Malware related to Log4Shell
- Specialized exploits to bypass authentication on D-Link devices.

INQUIRY: ATTACKS RECORDED BY HONEYPOTS

GEOGRAPHY OF ATTACKS

Main time zones:

- Asia/Shanghai - 40% of attacks
- Europe/Berlin - 33% of attacks.

The main attackers come from China, the United States, France, Taiwan, and Ukraine.

CHARACTERISTICS OF ATTACKING IPs

- Known malicious IPs (“Known attacker” reputation): 312 cases
- Botnets actively used for distributed attacks.

USE OF WEAK CREDENTIALS

Attackers frequently try to use **weak** or **default credentials**: passwords such as 123456, admin, password, and root dominate the password cloud.

INQUIRY: ATTACKS RECORDED BY HONEYPOTS

This investigation allowed us to draw some important conclusions about current trends in cyber attacks:

1. ATTACKS STILL EXPLOIT WELL-KNOWN VULNERABILITIES

Despite patches being available for vulnerabilities such as Log4Shell or CVE-2016-6563, many infrastructures remain exposed to these threats.

2. THE MAIN TARGETS ARE SERVERS and IoT DEVICES

The distribution of attacks highlights that systems with remote access and poorly configured devices are the most common targets.

3. THE SIMPLICITY OF THE HONEYPOT SETUP CAN DELIVER SIGNIFICANT RESULTS

Even with a basic configuration, it is possible to collect useful data to better understand the methods and strategies of attackers.

INQUIRY: ATTACKS RECORDED BY HONEYPOTS

4. THE IMPORTANCE OF CONTINUOUS MONITORING

The data collected shows that malicious activities evolve rapidly, underlining the need for continuous monitoring to keep abreast of new threats.

5. THE FUNDAMENTAL ROLE OF INFORMATION SHARING

Studies like this can contribute to a collective understanding of threats, strengthening defenses not only at the individual level, but also at the community level.

CONCLUSION

This investigation provided interesting data to analyze current threats, including the most frequently exploited vulnerabilities, the affected products, and the malicious techniques used. Although the results are not representative of all contexts, they offer a useful basis for further research and improved safety strategies. Understanding attack trends is essential for anticipating future threats and adapting protection measures accordingly.

2025 CYBERSECURITY CHALLENGES

2025 CYBERSECURITY CHALLENGES

After an extremely intense 2024, let's look at the **current cybersecurity challenges** for 2025 in the European context.
Firstly, it is useful to break down expectations into three main categories:

- **Challenges not to be underestimated**
- **Evolving new challenges**
- **Challenges to be prepared for**

As we look ahead to 2025, some classic cyberattacks that should not be underestimated and which we believe are once again on the rise include:

PHISHING: STILL CASTING A WIDE NET

Phishing is a type of online scam where cybercriminals try to dupe people, tricking them into providing sensitive personal information, such as passwords, credit card numbers, or bank details. This is often done through e-mails, text messages, or fake websites that mimic the appearance of legitimate companies or institutions.

2025 CYBERSECURITY CHALLENGES

Baiting, hooking and catching are the three steps of a phishing attack:

1. **Baiting**: The scammer sends a message, usually an e-mail or SMS, that seems to come from a reliable source (such as a bank, company, social network)
2. **Hooking**: The message contains a link or attachment which, if clicked, leads to a fake or malware-infected website
3. **Catching**: The fake website requests the entry of personal information, which is stolen by the scammer.

There are many different types of phishing such as:

- **Generic Phishing**: Targets a large number of people with generic messages.
- **Spear-phishing**: Targets specific individuals, often using personal information to make the attack more credible.
- **Whaling**: Targets high-profile figures, such as business executives or celebrities.
- **Smishing**: Uses SMS messages to trick victims.
- **Vishing**: Uses phone calls to obtain personal information.

2025 CYBERSECURITY CHALLENGES

The role of employees is fundamental in protecting against phishing attacks, as they are the **company's first firewall** capable of recognizing a phishing campaign through simple precautions:

- **Unexpected messages**: Be wary of e-mails or messages you aren't expecting, especially if they request personal information.
- **Grammatical errors**: Phishing messages often contain grammatical errors, although with the use of *Gen-AI* they are less frequent.
- **Suspicious links**: By hovering over the links without clicking, it is possible to preview a link and check if it is different from the one displayed.
- **Urgent requests**: Scammers often apply pressure to get information quickly.
- **Missing information**: A legitimate company will never ask you for information they already have; simply cross-check before responding.

2025 CYBERSECURITY CHALLENGES

INFOSTEALER: SILENT MALWARE

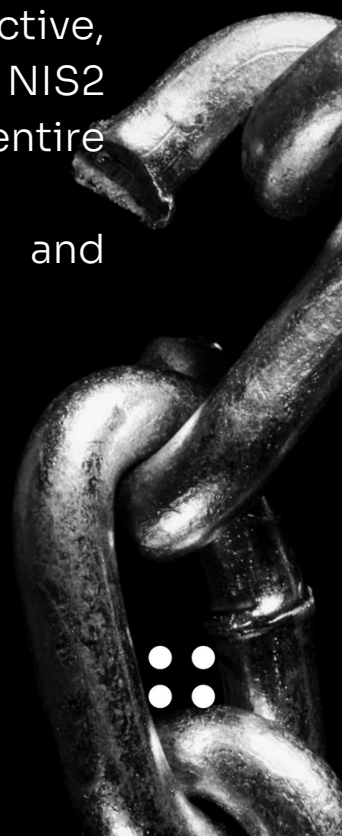
In Europe, **malware** is one of the preferred techniques used by cybercriminals, and **infostealers** account for 78% of the most widespread malware types. Infostealer malware is specialized in the systematic theft of **personal data** (Cert-Agid Report, 2023). The danger lies in their ability to operate in the shadows, silently collecting credentials, session cookies, and credit card data. The simplest ones steal information from web browsers, such as Google Chrome, Mozilla Firefox, and others based on Chromium. They are also able to steal files from desktops and other folders, cryptocurrency wallets, and multi-factor authentication (MFA) extensions. Once stolen, this data allows criminals to perfectly impersonate victims, gaining access to their bank accounts, e-mails, and even corporate networks. It is comprehensive digital identity theft that can have devastating consequences for both individuals and organizations.

2025 CYBERSECURITY CHALLENGES

Looking ahead to 2025, we expect several emerging challenges that are likely to gain traction, including:

THIRD-PARTY RISK MANAGEMENT

Managing the risks related to **third-party suppliers** has become a priority, so much so that it is becoming common practice for companies to sign stringent contractual security clauses in supply relationships. Dependence on **third parties** (such as vendors, suppliers, partners, contractors or service providers) creates a chain of vulnerabilities that is difficult to control. The risk is amplified by the fact that a supplier with weak security can serve as an entry point for attacking even the most well-protected organizations, as demonstrated by numerous supply chain attacks. Lawmakers are also moving in this direction: In 2024, and from January 17, 2025, the security of third parties became mandatory both under the DORA Directive, which involves financial systems, and under the NIS2 Directive, which focuses on the security of the entire supply chain.
Therefore, it is a priority to manage, identify, and reduce the risks related to the use of third parties.



2025 CYBERSECURITY CHALLENGES

GENERATIVE AI: A WEAPON IN THE ARSENAL OF CYBERCRIMINALS

Generative artificial intelligence has become a double-edged sword. While on the one hand, it has accelerated automation and technological development across industrial sectors (as we saw recently with the launch of *Sora AI*, which promises to revolutionize the film industry), on the other, it has also benefited the activities of cybercriminals. The risk lies in its ability to automate the creation of **ultra-convincing phishing attacks**, generate polymorphic malware that evades antivirus detection, and even discover new vulnerabilities in systems.

2025 CYBERSECURITY CHALLENGES

GENERATIVE AI: A WEAPON IN THE ARSENAL OF CYBERCRIMINALS

The CYBEROO Observatory found increased sophistication in deepfake-based **scam** attempts with fake videos or audio. A recent scam used a deepfake of a CEO to get a fund transfer from a large tech company. What's more, even **Large Language Models** are not immune from attacks. Like any complex system, they could have vulnerabilities and be exploited by threat actors to access company information or carry out targeted attacks. This was confirmed by the discovery of some vulnerabilities in the DeepSeek or Microsoft Copilot system, underlining how crucial it is to address the security of large language models (CVE-2024-43610; CVE-2024-49038). An attack targeted at these vulnerabilities could lead to the disclosure of confidential information or manipulation of the responses generated by the model.

2025 CYBERSECURITY CHALLENGES

PASSWORDLESS: A FUTURE WITHOUT PASSWORDS—RISKS AND BENEFITS

Access management is evolving beyond the traditional **password** system. Gartner predicts that by 2027, over 75% of workforce authentication transactions and more than 40% of customer authentication transactions will be passwordless, resulting in significant improvements in security and user experience (Gartner, 2024). The Zero Trust approach is no longer an option but a necessity, with biometric authentication and hardware tokens taking the place of the beloved “Password123!”. However, it is important to consider that alternative authentication systems could become the target of increasingly sophisticated attacks, aimed at cloning fingerprints or compromising security tokens. In practical terms, hackers could install malware specifically designed to intercept one-time passcodes (OTPs). Or they could inject Trojans into web browsers to intercept shared data, such as unique access codes or magic links.

2025 CYBERSECURITY CHALLENGES

QUISHING: PHISHING IN A QR CODE DISGUISE

Quishing (QR Code phishing) is emerging as the new frontier in social engineering. Unlike traditional phishing that relies on e-mails or messages, Quishing uses malicious QR codes to redirect victims to fraudulent websites or to download malware. Attacks based on malicious QR Codes increased by 587% in the second half of 2023. Its spread became apparent in 2024, especially in Switzerland, where various scams emerged, ranging from one using the postal service to fake letters seemingly from the Federal Office of Meteorology and Climatology. In 2025, Quishing is expected to become one of the main attack vectors in the social engineering threat landscape. Therefore, it is important to pay close attention to the QR Codes you scan using your smartphone.

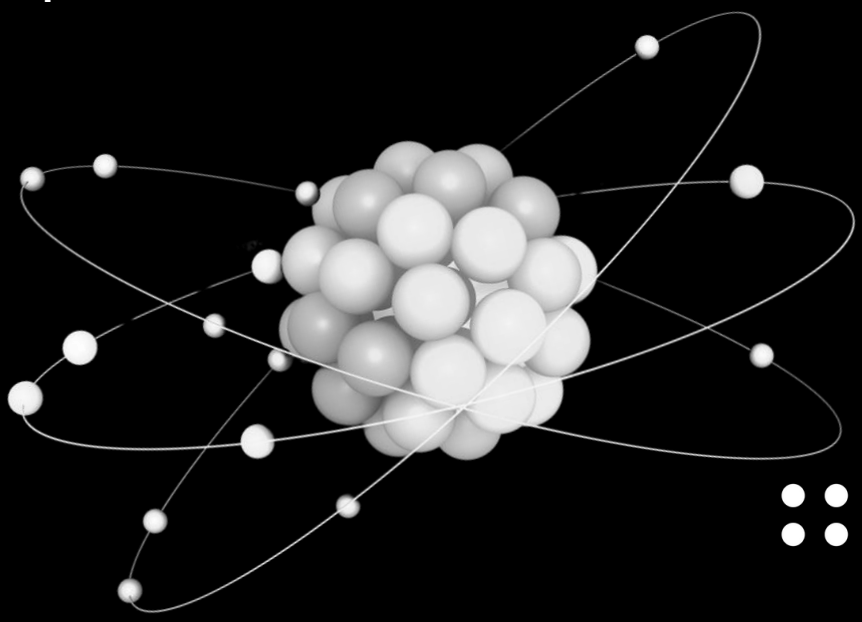
This QR Code, however,
is safe to scan.

2025 CYBERSECURITY CHALLENGES

We have identified two main challenges to be prepared for in the near future:

QUANTUM ATTACKS: A THREAT TO ENCRYPTION

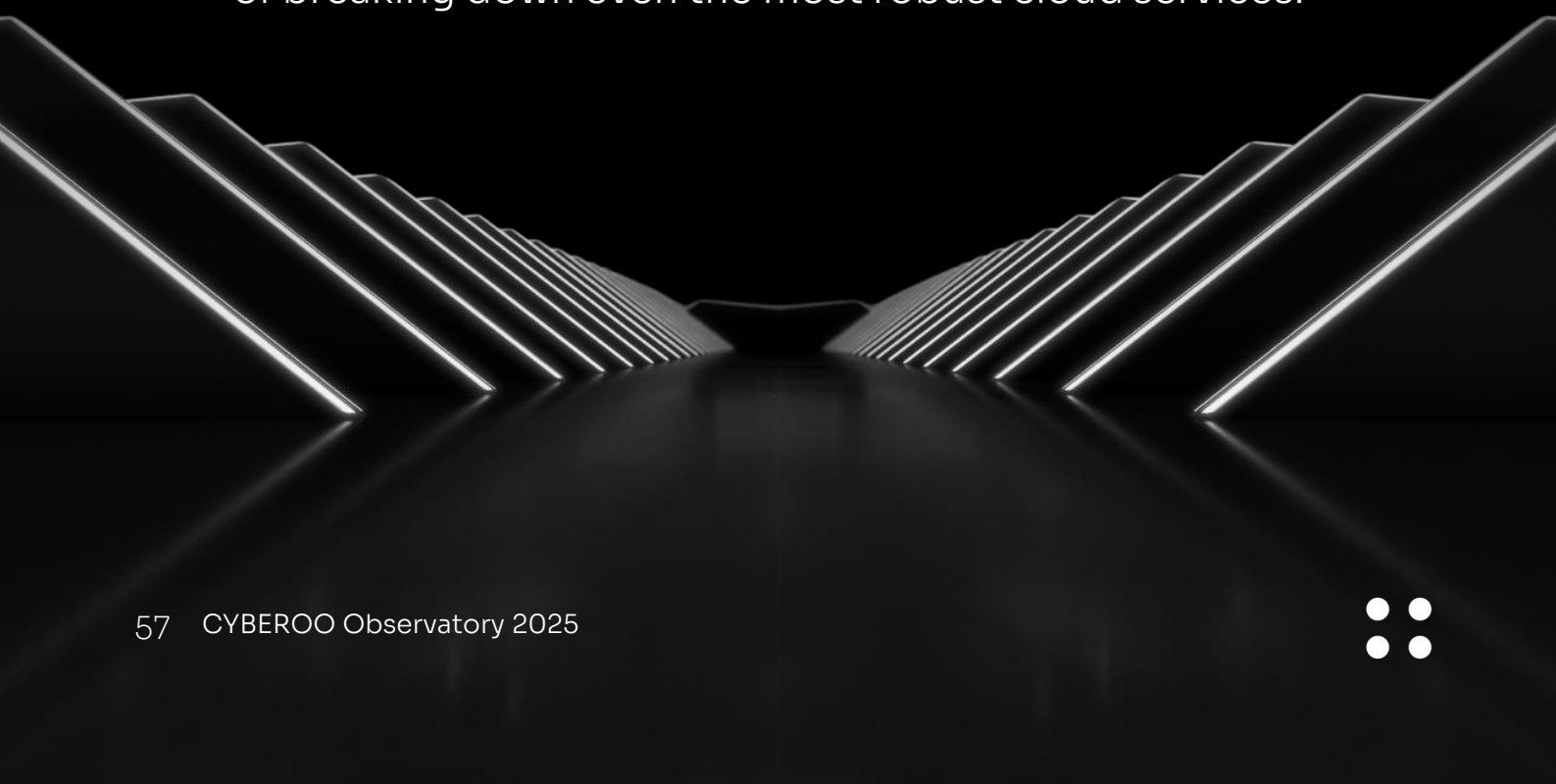
One of the fastest-growing technologies in recent years is **quantum computing**: a technology that applies the laws of quantum physics to potentially solve complex problems much faster than traditional computers. It would take the crystal ball to know if there will be effective deployment of this technology in 2025. However, this development certainly represents **a threat to cybersecurity**. The danger is real: when quantum computers become widespread enough, they will be able to decrypt most of the cryptographic systems in use today. This means that sensitive data, secure communications, and financial transactions will become vulnerable, requiring a complete overhaul of security systems. The banking sector is particularly exposed and is testing new cryptographic algorithms to counter possible **quantum attacks**.



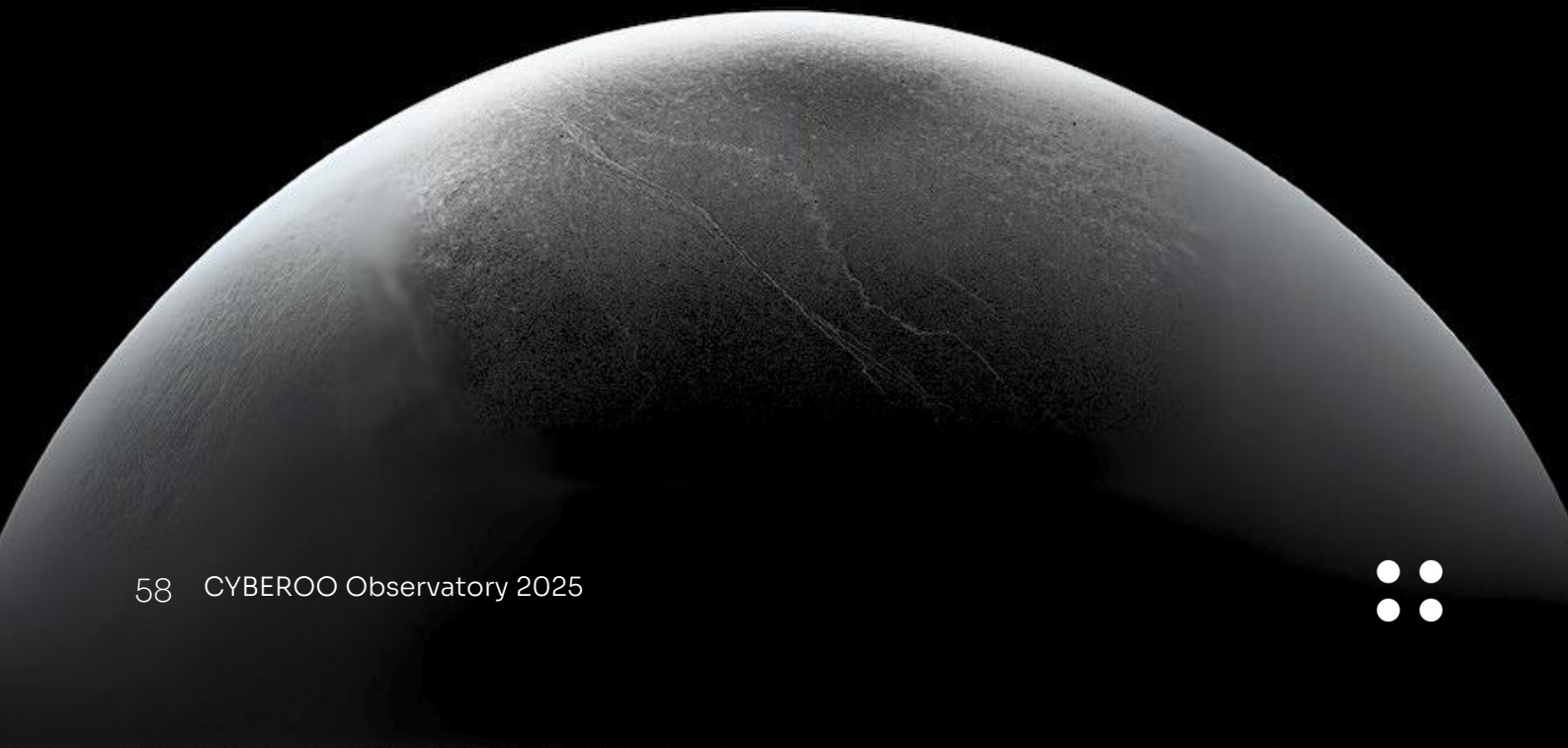
2025 CYBERSECURITY CHALLENGES

INTERNET OF THINGS & CYBERSECURITY: A DELICATE BALANCE

Today we are facing a massive growth in **IoT devices** that, according to estimates, will see a presence of over 55.7 billion devices by 2025 capable of generating almost 80B zettabytes of data (International Data Corporation). These devices, often designed with a greater focus on smart features than on **security by design**, are exploited by criminal gangs to launch devastating DDoS attacks, which can severely damage corporate IT infrastructures.
The threat exists across multiple levels: on the one hand, IoT devices with weak security become easy access points to infiltrate corporate networks; on the other, once compromised, they are enlisted in botnets that can generate traffic volumes in the order of terabits per second, generating DDoS attacks capable of breaking down even the most robust cloud services.



HOW TO DEFEND AGAINST CYBER ATTACKS IN 2025



HOW TO DEFEND AGAINST CYBER ATTACKS IN 2025

INTRODUCTION BY LUCA BONORA - CYBEROO EVANGELIST

As cybercriminals hone their techniques, companies must adopt **defense** and **response** strategies to protect their data and infrastructures on equal terms. Defense strategies that were effective until recently may no longer be effective today. To effectively prevent and mitigate cyber attacks in the cyberspace of 2025, it is necessary to start with a few simple but important questions:

- How would you know if you were under attack?
- What are the potential cyber threats to your company and employees?
- How would you react in the event of an actual attack?
- What processes have you defined to raise your resilience level?
- How would you identify an attack coming from a trusted supplier?
- What kind of support and training do you provide to company employees?

In 2025, we are facing a gradual increase in the operational capabilities of **Artificial Intelligence**, as we have often mentioned in this report. On that point, I wonder whether AI will ever be capable of genuine “new reasoning.” Technological developments lead us to believe that this might become possible before long.

HOW TO DEFEND AGAINST CYBER ATTACKS IN 2025

INTRODUCTION BY LUCA BONORA - CYBEROO EVANGELIST

That said, I'm certain that humans are developing infrastructures tailored to artificial intelligence, enabling AI to perform operations and tasks more efficiently, at greater speed, and with higher consistency than 80% of humans. This turns out to be **the most significant and fastest evolution** that humans have ever encountered to date in the history of humanity. It would be superficial, and like burying your head in the sand, not consider and acknowledge that even in the world of organized cybercrime, increasingly faster and more effective tactics, techniques, procedures, and attack technologies are being developed. This requires infrastructure managers, as well as those responsible for the company's business, to increase and improve their ability **to monitor, detect, and respond continuously and efficiently to new attacks**. That is why the CYBEROO Observatory was established, providing an extraordinary and increasingly recognized point of reference to help companies reflect on their maturity level and the plan the necessary steps to strengthen their culture, awareness, and the security of their business infrastructures. The aim is to increase corporate security and resilience by 2025. Let's see how.

HOW TO DEFEND AGAINST CYBER ATTACKS IN 2025

1. IMPLEMENT 24/7 MONITORING AND RESPONSE SYSTEMS

The implementation of **24/7 monitoring and response systems** allows you to guarantee proactive and continuous protection of digital infrastructures. These systems integrate advanced artificial intelligence and machine learning technologies with the skills of a 24h I-SOC team to **analyze data flows in real time**, identifying anomalies that could indicate malicious activity. Immediate response capability allows threats to be quickly mitigated, reducing exposure time, and limiting potential damage. The effectiveness of such systems depends on their ability to **dynamically adapt** to new types of attacks, through constant updates based on Threat Intelligence.

HOW TO DEFEND AGAINST CYBER ATTACKS IN 2025

2. MANAGE RISK WITH CYBER THREAT INTELLIGENCE

You cannot consider your infrastructure secure without constantly monitoring the threats that lurk in the depths of the **Deep** and **Dark Web**. Cyber risk management also relies on the use of **Threat Intelligence** to anticipate and mitigate cybercrime threats. The collection and analysis of data related to ongoing malicious activities allows organizations to identify potential vulnerabilities and take preventive measures. The integration of Threat Intelligence in strategic decision-making processes allows development of a proactive approach to security, improving the ability to respond to incidents and optimizing the allocation of security resources. This systematic approach to risk management is essential to effectively address the ever-changing threat landscape.

HOW TO DEFEND AGAINST CYBER ATTACKS IN 2025

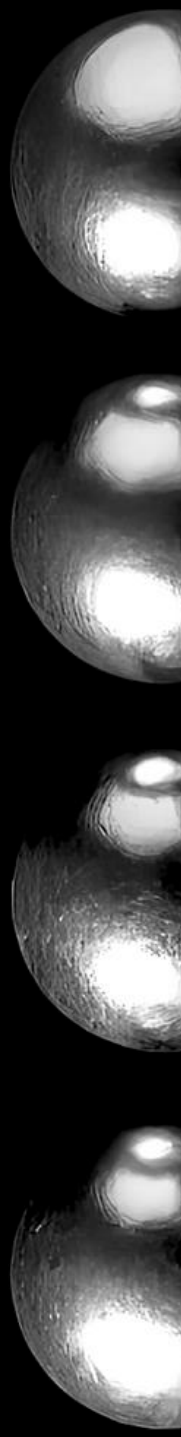
3. BEYOND DETECTION: THE IMPORTANCE OF REMEDIATION

In recent months, many companies have invested in Detection to counter cyber threats. It must, however, be considered that the truly critical element in the management of cybersecurity incidents is the **Remediation** phase: Concrete action to remediate the weaknesses identified in the Detection phase in the cybersecurity system. Once the Detection phase is complete, it is imperative to adopt Remediation strategies that are quick and effective to restore the security of compromised systems. This process includes **identifying exploited vulnerabilities**, **applying corrective patches**, and **reviewing security policies** to prevent future breaches. The systematic approach to Remediation with a certified incident response process not only mitigates the immediate effects of an attack but also contributes to the continuous improvement of the organization's security framework.

HOW TO DEFEND AGAINST CYBER ATTACKS IN 2025

4. PREPARE A CYBERSECURITY AND INCIDENT RESPONSE STRATEGY

Developing an **effective cybersecurity strategy** is the basis for protecting against cyber attacks. As we will see in the next point, a key aspect of this strategy is the development of proactive security processes which allow potential vulnerabilities to be identified before they can be exploited. As with the company emergency and evacuation plan, there must be a detailed **Incident Response Plan** in place in advance, which includes procedures for rapid incident detection, containment, elimination of threats, and restoration of normal operations. These plans must be regularly tested and updated to take into account new threats and technological developments. At CYBEROO, this entire process is coordinated by the Security Advisor Manager (SAM).



HOW TO DEFEND AGAINST CYBER ATTACKS IN 2025

5. IMPROVE THE SECURITY OF THE ENTIRE PRODUCTION CHAIN

In 2025, it is essential to improve the **supply chain** by regularly monitoring **suppliers and third parties**, and requiring them to comply with security standards. In detail, it is important to implement **strict controls**, adopt measures such as **periodic audits, detailed risk assessments** and the **integration of security clauses** in contracts. These actions will help ensure that every link in the supply chain maintains an adequate level of security, thereby reducing the likelihood of compromises that could have devastating effects on business infrastructure.

HOW TO DEFEND AGAINST CYBER ATTACKS IN 2025

6. SECURITY AWARENESS: STRENGTHEN HUMAN KNOWLEDGE

Creating a **safety culture** within an organization is a complex and long-term process that requires an ongoing commitment in terms of training and awareness raising. **Security Awareness** must be integrated at all levels of the company, promoting a thorough understanding of cyber threats and security practices among employees. Regular training programs, attack simulations, and updates on the latest threat trends are critical tools for developing a security mindset. Only through a **deep-rooted cultural change** is it possible to achieve a proactive and resilient defense against cyber threats.

CYBEROO

THE IMPORTANCE OF A PROACTIVE APPROACH

THE IMPORTANCE OF A PROACTIVE APPROACH

Running on adrenaline for too long isn't sustainable. A **proactive process** helps prevent escalation and reduces stress for both the cybersecurity team and the company. CYBEROO emphasizes the importance of this approach, which goes beyond simple technological implementation, allowing companies to consider outsourcing as a key element of cybersecurity management. Through a Managed Detection & Response (MDR) service, it provides a 24/7 I-SOC team that continuously manages monitoring, analysis and response to threats, ensuring continuous coverage, at any time.

This process combines sophisticated Threat Intelligence mechanisms with timely action when anomalies emerge, ensuring that there are no shadow zones in the protection of digital infrastructures. In this way, the company can focus on its business, while the CYBEROO team is protecting it 24 hours a day, 365 days a year by deploying cutting-edge technology and specialist skills.

ABOUT US

CYBEROO is a European cybersecurity vendor, proudly rooted in Italy, specialized in defending against cybercrime. As a pioneer in the European cybersecurity landscape, CYBEROO is proud to be the first cybersecurity company to be listed on the Italian Stock Exchange since 2019 – and the only Italian MDR vendor in world to be named a “Representative Vendor” in the Gartner® Market Guide for Managed Detection and Response Services. By choosing CYBEROO, businesses are not only investing in robust cybersecurity measures but also aligning themselves with a company that embodies European values of quality, reliability, and innovation.

EXTERNAL SOURCES CONSULTED

- “2024 Report on the State of the Cybersecurity in the Union”, © European Union Agency for Cybersecurity (ENISA)
- "Cybercrime to cost the world $10.5 trillion annually by 2025", Intrusion inc.
- Clusit Report October 2024
- "Summary Report on the Trends of Malicious Campaigns Affecting Italy in 2023", Cert-Agid
- EU Directive 2022/2555 (NIS 2)
- Dora Directive, Official Journal of the European Union of December 27, 2022
- Microsoft Copilot Vulnerabilities, CVE.org
- "Migrate to passwordless authentication to enhance security and optimize ux", Gartner
- Raheman, F. The Future of Cybersecurity in the Age of Quantum Computers. Future Internet 2022, 14, 335
- "Future of Industry Ecosystems: Shared Data and Insights", International Data Corporation

CONTACT US

Cyberoo S.p.A.
Via Brigata Reggio, 37, 42124, Reggio Emilia, Italy

tel. +39 0522 388111

www.cyberoo.com

CONTACT US

CYBEROO