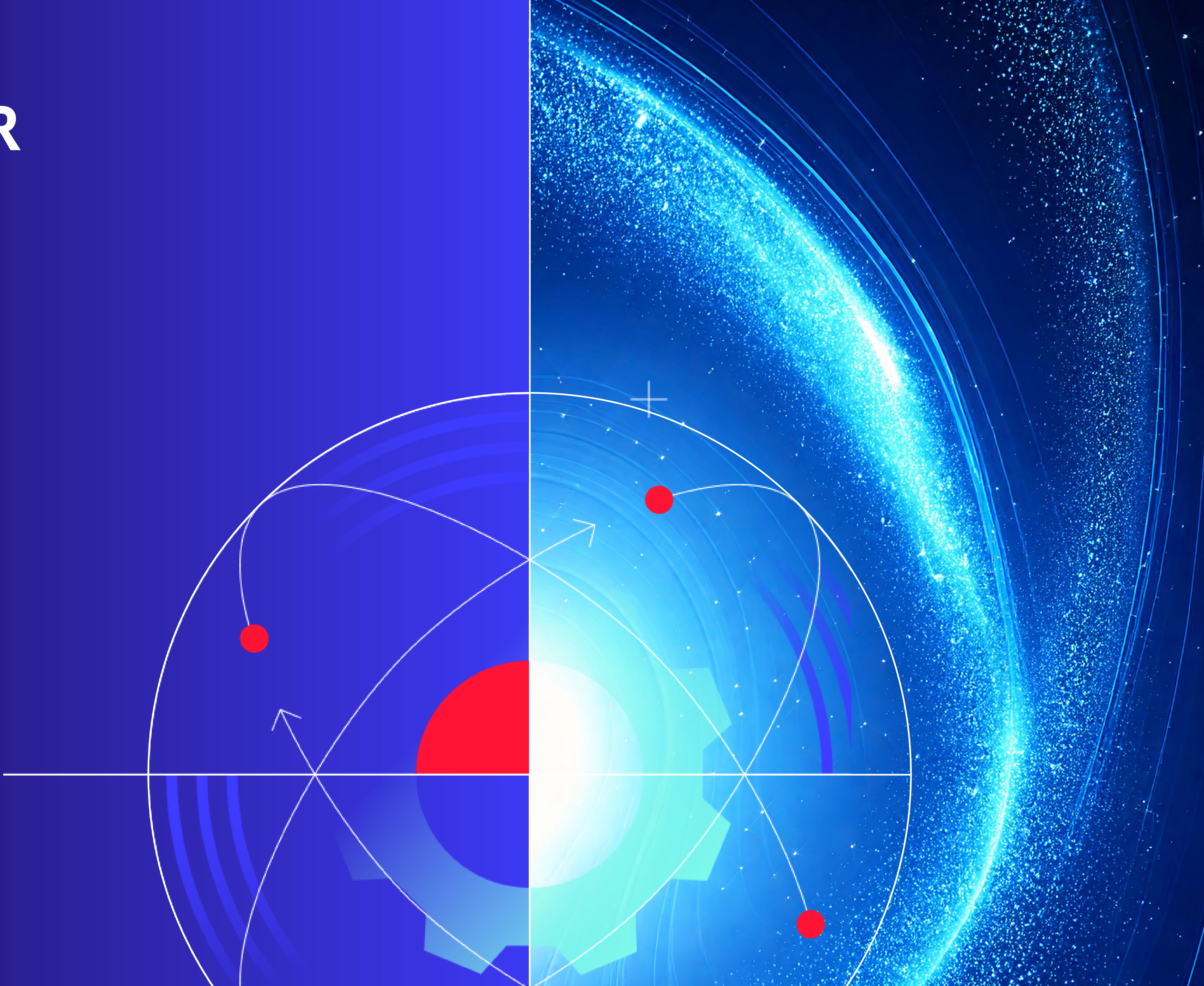
GATEWATCHER

2024 *Cyberthreat Landscape_*



*Abstract_*

A publication by

PURPLE TEAM
GATEWATCHER

Introduction_

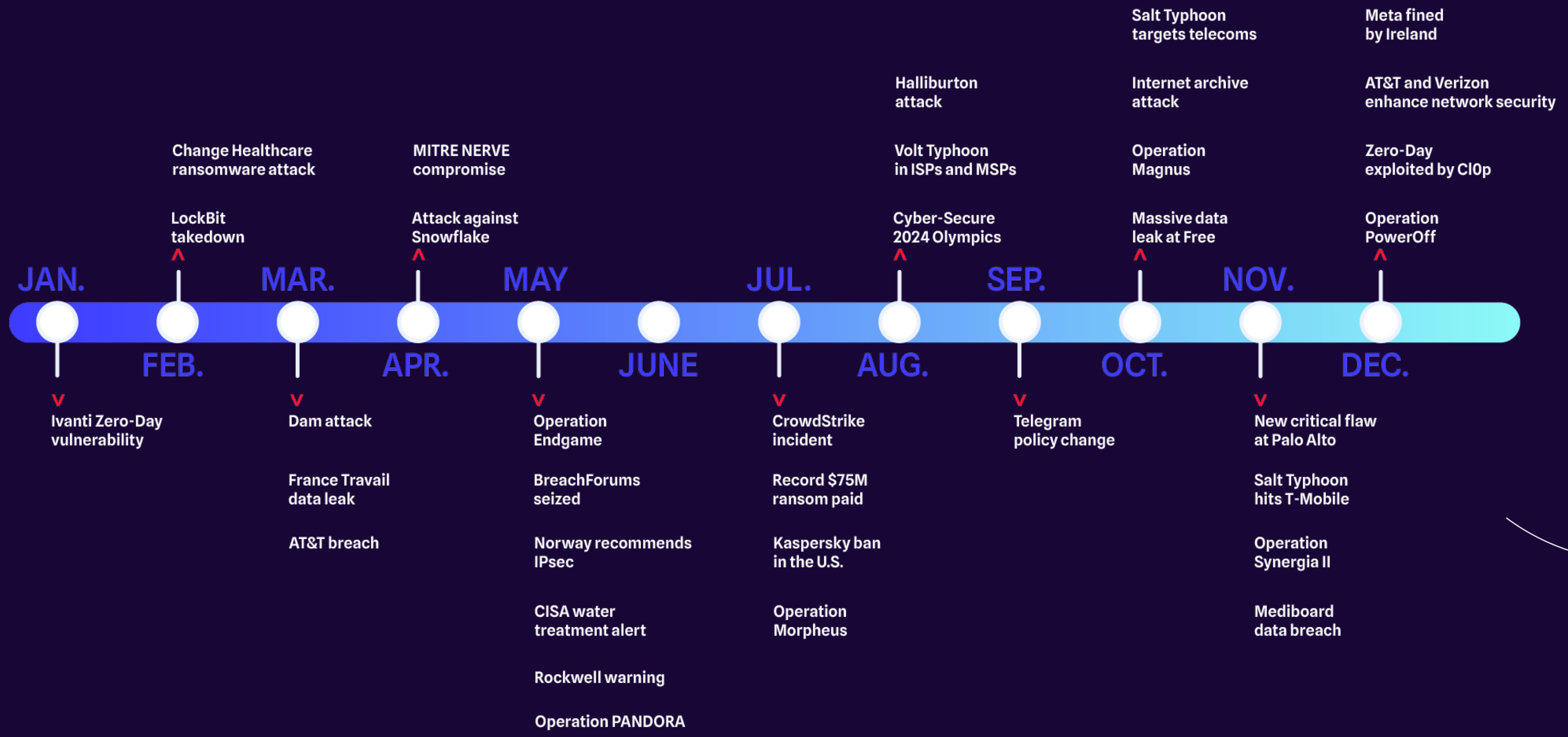
For the 2024's edition of the Cyberthreat Landscape, Gatewatcher's Purple Team presents its analysis of the cyber threats that marked the year 2024. Based on data collected by our CTI platform and monitoring efforts carried out by our analysts, this CTAR aims to shed light on key developments observed over the course of 2024 in the cyber threat landscape and its main actors.

At Gatewatcher, the Purple Team plays a key role in identifying, analyzing, and understanding the threats facing organizations. Composed of specialists in Cyber Threat Intelligence, incident response, and penetration testing, the team contributes to the continuous improvement of our network detection solutions and the anticipation of emerging threats.

The year 2024 was marked by significant changes in the tactics used by cybercriminals, combining technical sophistication and strategic opportunism. While stealers overtook ransomware in terms of volume, ransomware groups adapted by diversifying their business models and strengthening their resilience to takedown actions. Meanwhile, attacks targeting industrial infrastructure and major international events surged, focusing on critical sectors and high-profile targets such as the 2024 Paris Olympic Games.

At the same time, the exploitation of vulnerabilities accelerated, further shrinking the window between discovery and active exploitation. Phishing and quishing, fueled by artificial intelligence, became increasingly sophisticated, making fraudulent campaigns more convincing and harder to detect. These developments reflect a constantly evolving cyber landscape, where the speed at which attackers adapt demands constant vigilance from defenders.

This report aims to provide a concise overview of the key threats observed in 2024 and analyze their impact on businesses and institutions. By documenting these trends and detailing adversary strategies, Gatewatcher's Purple Team offers essential insights to better understand and anticipate emerging cyber risks.



JAN.

Ivanti Zero-Day vulnerability

FEB.

Change Healthcare ransomware attack

LockBit takedown

MAR.

Dam attack

France Travail data leak

AT&T breach

APR.

MITRE NERVE compromise

Attack against Snowflake

MAY

Operation Endgame

BreachForums seized

Norway recommends IPsec

CISA water treatment alert

Rockwell warning

Operation PANDORA

JUNE

JUL.

CrowdStrike incident

Record $75M ransom paid

Kaspersky ban in the U.S.

Operation Morpheus

AUG.

Halliburton attack

Volt Typhoon in ISPs and MSPs

Cyber-Secure 2024 Olympics

SEP.

Telegram policy change

OCT.

Salt Typhoon targets telecoms

Internet archive attack

Operation Magnus

Massive data leak at Free

NOV.

New critical flaw at Palo Alto

Salt Typhoon hits T-Mobile

Operation Synergia II

Mediboard data breach

DEC.

Meta fined by Ireland

AT&T and Verizon enhance network security

Zero-Day exploited by Cl0p

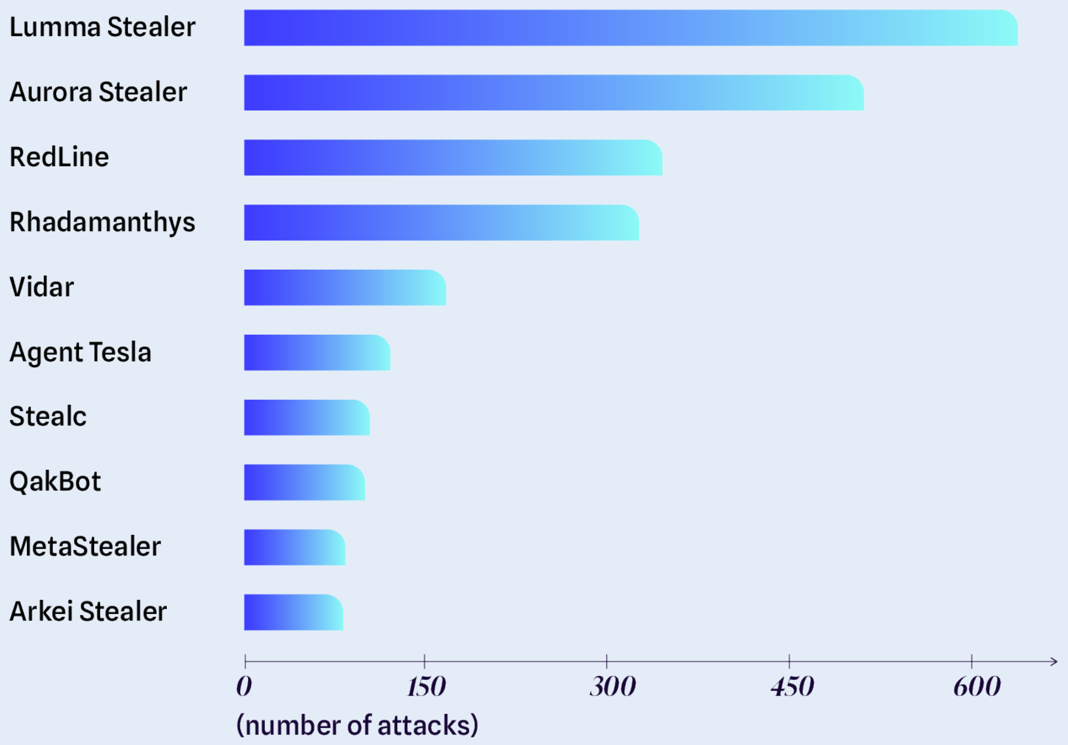
Operation PowerOff

01

MAIN THREATS_

Stealers: A rising threat in 2024

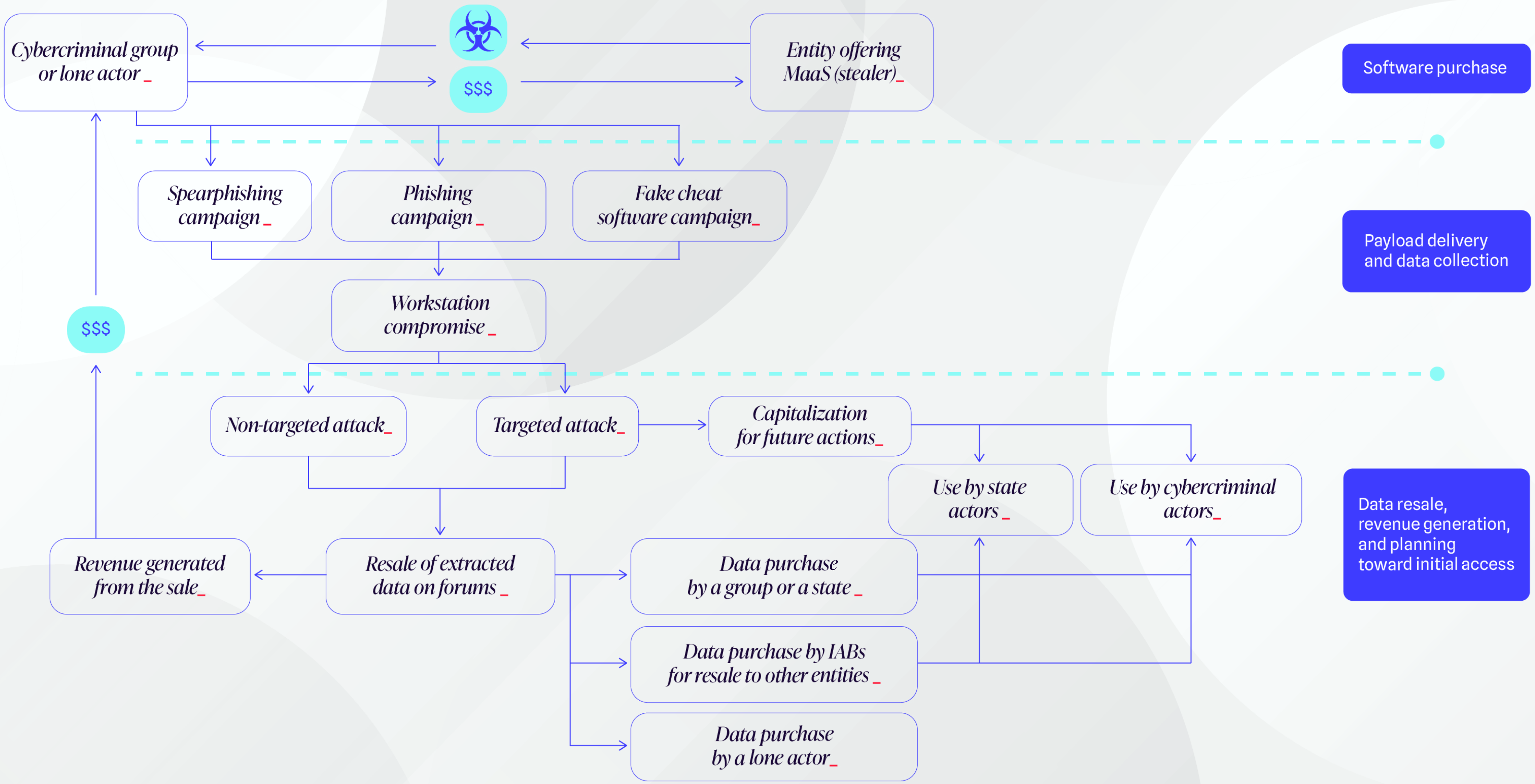
TOP10 Malwares 2024_



In 2024, a significant shift occurred in the malware landscape. While ransomware previously dominated, infostealers - or simply "stealers"- took center stage among the most commonly observed types of malware. This trend is supported by a sharp increase in publications on the subject, growing communication from actors selling such services, and the rise in data leak sales on underground forums.

As a reminder, stealers are malicious software programs specialized in stealing user data. They target a wide range of information, from banking details to streaming service accounts. Each variant has its own features, such as the ability to replace clipboard content or self-delete after extracting the information.

Use of stealers_


Cybercriminal group or lone actor_
$$$
Entity offering MaaS (stealer)_
Software purchase
Spearphishing campaign_
Phishing campaign_
Fake cheat software campaign_
Workstation compromise_
Payload delivery and data collection
$$$
Non-targeted attack_
Targeted attack_
Capitalization for future actions_
Use by state actors_
Use by cybercriminal actors_
Revenue generated from the sale_
Resale of extracted data on forums_
Data purchase by a group or a state_
Data purchase by IABs for resale to other entities_
Data purchase by a lone actor_
Data resale, revenue generation, and planning toward initial access

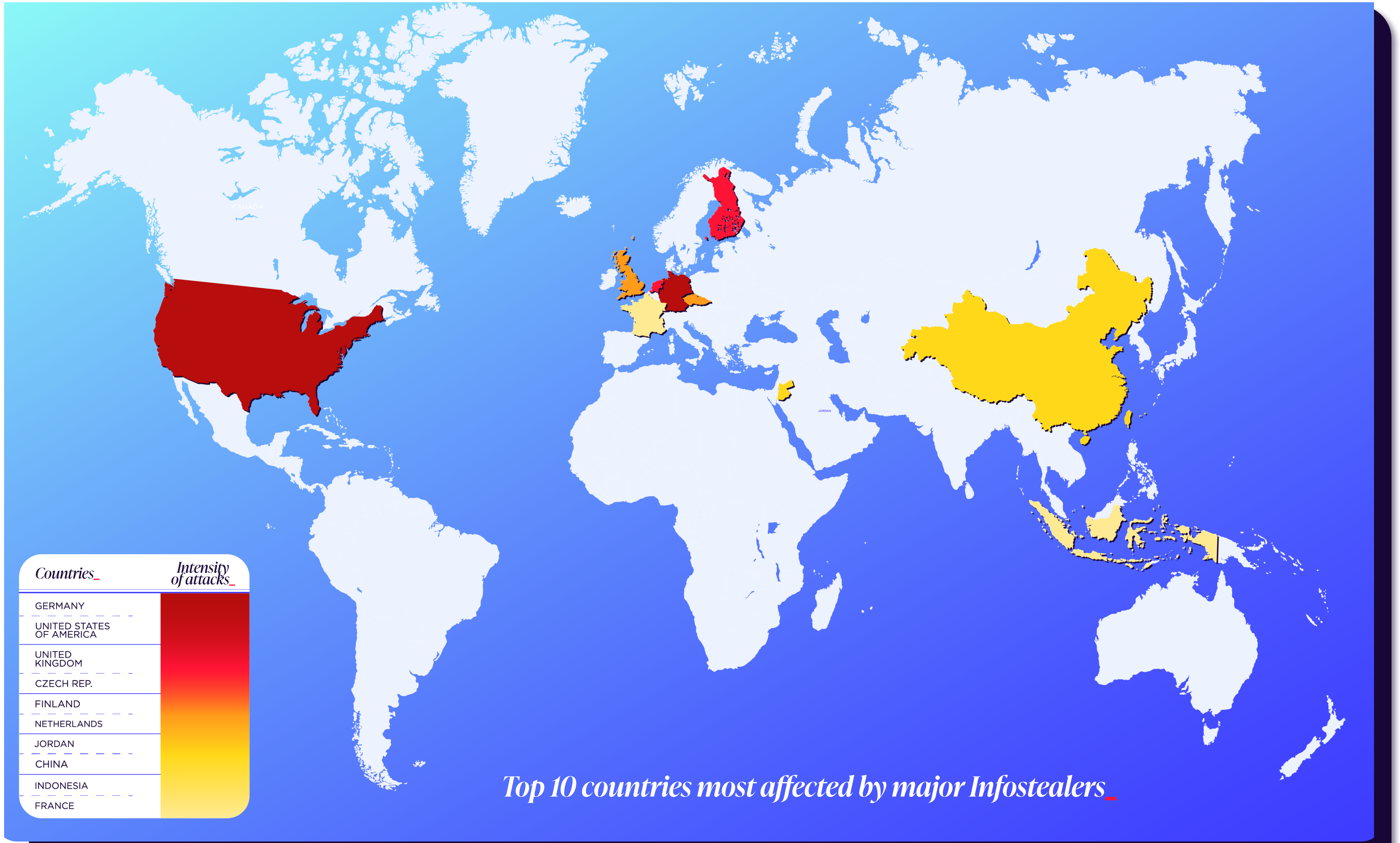
Targets_

Unless involved in specifically tailored campaigns, stealers do not typically target particular entities. Most actors aim to maximize profitability by amassing and reselling large credential dumps - often containing millions of entries.

This random targeting, paired with the diverse range of stealer groups, complicates profiling malicious actors. Even smaller groups that focus on individuals can pose a serious threat by reselling access to more organized cybercriminals.

Buyers of these services include cybercriminals, state-affiliated groups, and lone actors. While these tools are often distributed through hijacked services, some high-profile campaigns emerged in 2024.

A notable example was the widespread deployment of Lumma Stealer during the League of Legends World Championship. Here, a malvertising campaign leveraged the event's hype to trick players into downloading malware disguised as the game's installer.



*Top 10 countries most affected by major Infostealers_*

The global distribution of victims affected by the most prevalent stealers in 2024 illustrates the wide reach of this threat. However, many of these malware strains include checks to determine whether the infected system is located in a **Commonwealth of Independent States (CIS)** country. If so, the malware payload is typically deactivated—explaining the limited impact observed in those regions.

*The data*_

Contrary to popular belief, all stolen data has value and can be monetized. Some uses are obvious, such as obtaining login credentials for online services or accessing banking information. However, even a low-balance bank account can be useful, for instance, in money laundering schemes.

Another major reason for harvesting massive amounts of credentials is to use them in "**credential stuffing attacks**" - automated login attempts using stolen username-password pairs on a large scale. Despite growing awareness, many users still reuse the same password across multiple services, including professional accounts.

It is crucial to understand that gaining access - even to a non-privileged system - represents a significant step for an attacker, opening the door to numerous possibilities. This reality is well understood by threat actors, who can exploit seemingly harmless credentials, as demonstrated by the data breaches at Okta, General Motors, and Levi's.

*Business model*_

In the cybercrime ecosystem, stealers are akin to a goose that lays golden eggs, present at every level of the value chain. They lie at the heart of a structured ecosystem - from developers who create the malware to resellers who monetize the stolen data.

Most stealers follow a **Malware-as-a-Service** (MaaS) model, offering various subscription tiers. For example, Lumma Stealer offers packages ranging from $250 for the "experienced" plan to $1000 for the "corporate" plan, which includes more advanced evasion techniques.

The raw stolen data, commonly referred to as "logs," has multiple uses. Some logs are freely accessible through various channels, while others - typically the most valuable - are sold on specialized forums or offered as part of subscription-based services.

The profit chain doesn't end there. Some more daring or technically skilled attackers use this data to gain access to various systems. These actors are known as **Infrastructure Access Brokers** (IABs), selling access to third parties, who may then use it for espionage or to launch ransomware attacks.

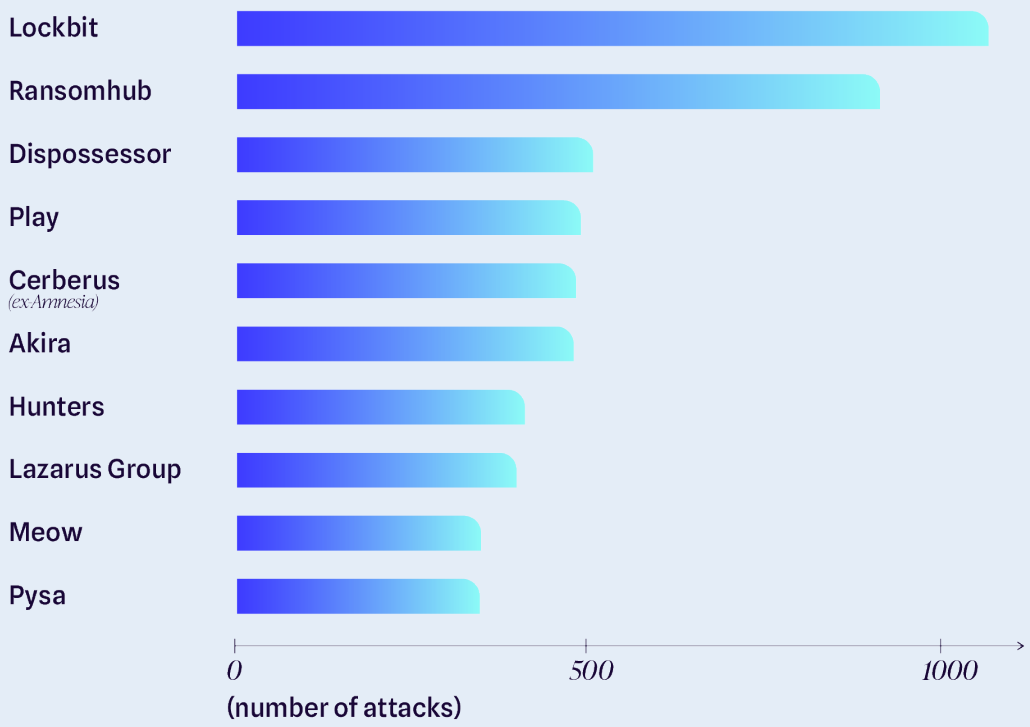
In conclusion, 2024 saw the rise of stealers as a major threat in the cybersecurity landscape, highlighting the ongoing evolution of malicious actor tactics and the need for increased vigilance in protecting both personal and corporate data.

Ransomware

In 2024, the rise of stealers should not overshadow the continued activity of ransomware, which still accounts for a significant portion of global cyberattacks.

This section highlights two key players in the current landscape. Lockbit, on one hand, remains one of the most active **Ransomware-as-a-Service** (RaaS) groups, achieving record profits despite international operations aimed at dismantling it. On the other hand, Cl0p, while not among the most prolific groups in terms of attack volume, has a unique operational model, and its actions since the end of 2024 warrant specific attention.

TOP10 Most active ransomware groups_



*Lockbit and operation CRONOS: A remarkable resilience_*

Before diving into the details of Lockbit's actions and its resilience, it's worth briefly revisiting Operation CRONOS. This joint operation, launched in February 2024 by ten countries, aimed to put an end to the activities of the Lockbit group. To achieve this, law enforcement agencies carried out arrests of suspected members, seized infrastructure belonging to the group, confiscated cryptocurrency assets, and recovered decryption keys that allowed victims to regain access to their data.

As of now, two arrest warrants have been issued for Russian nationals, arrests have taken place across several European countries, over 1,000 decryption keys have been recovered, and 200 cryptocurrency accounts have been seized. Nevertheless, the group's ability to withstand these actions highlights the complexity of dismantling such criminal organizations.

*Factors Behind the Group's Resilience_*

Several factors explain Lockbit's ability to continue operating despite the actions taken against it:

> **An efficient RaaS model:** Roles are segmented, and affiliates rotate regularly, allowing for diversification in operational methods.

> **Continuous evolution for greater resilience:** All components of the Lockbit ecosystem work together to evolve technically, tactically, and strategically.

> **"Best practices" inspired by the corporate world:** The group implemented an internal bug bounty program to improve the security of its tools and infrastructure.

What impact did operation CRONOS have?_

Operation CRONOS still had several important consequences:

> It ended Lockbit's monopoly, allowing other groups such as AlphaV/Blackcat to gain traction in the ransomware landscape.

> More concerningly, it led to the removal of previously enforced rules forbidding attacks on public or healthcare infrastructure. While these rules weren't always followed, they acted as a form of moral boundary for some affiliates.

*Cl0p: A multifaceted actor_*

Including Cl0p in this report may seem surprising, as the group was not particularly active until mid-December 2024.

However, Cl0p is far from just another Russian-speaking ransomware group. Tracing back to its origins, Cl0p is the ransomware "branch" of TA505, a criminal organization known for offering services such as phishing, stealers, and financial fraud.

Its organizational structure resembles that of mafia or cartel-style operations, diversifying criminal activities to maximize profit. This multi-disciplinary approach has also led to collaborations with other well-known actors, like FIN11. This operational variety may also explain the group's long periods of silence between attacks. In fact, after its attack on MoveIT in 2023, Cl0p remained mostly inactive until late 2024, when it struck again - this time targeting Cleo, another secure file transfer platform.

*Strategic similarities in the attacks_*

Both attacks shared several strategic characteristics:

> They targeted the supply chain.

> They exploited zero-day vulnerabilities.

> They impacted systems used by large corporations, resulting in major consequences due to the sensitive data involved.

This modus operandi allows Cl0p to demand high ransom payments, likely enabling the group to operate without needing to launch additional attacks for extended periods - buying time to develop new exploitation techniques.

Cl0p is a group worth monitoring closely. Even if it appears dormant following the attack on Cleo's software platform, it could resurface at any time and potentially cause millions of dollars in damages.

02

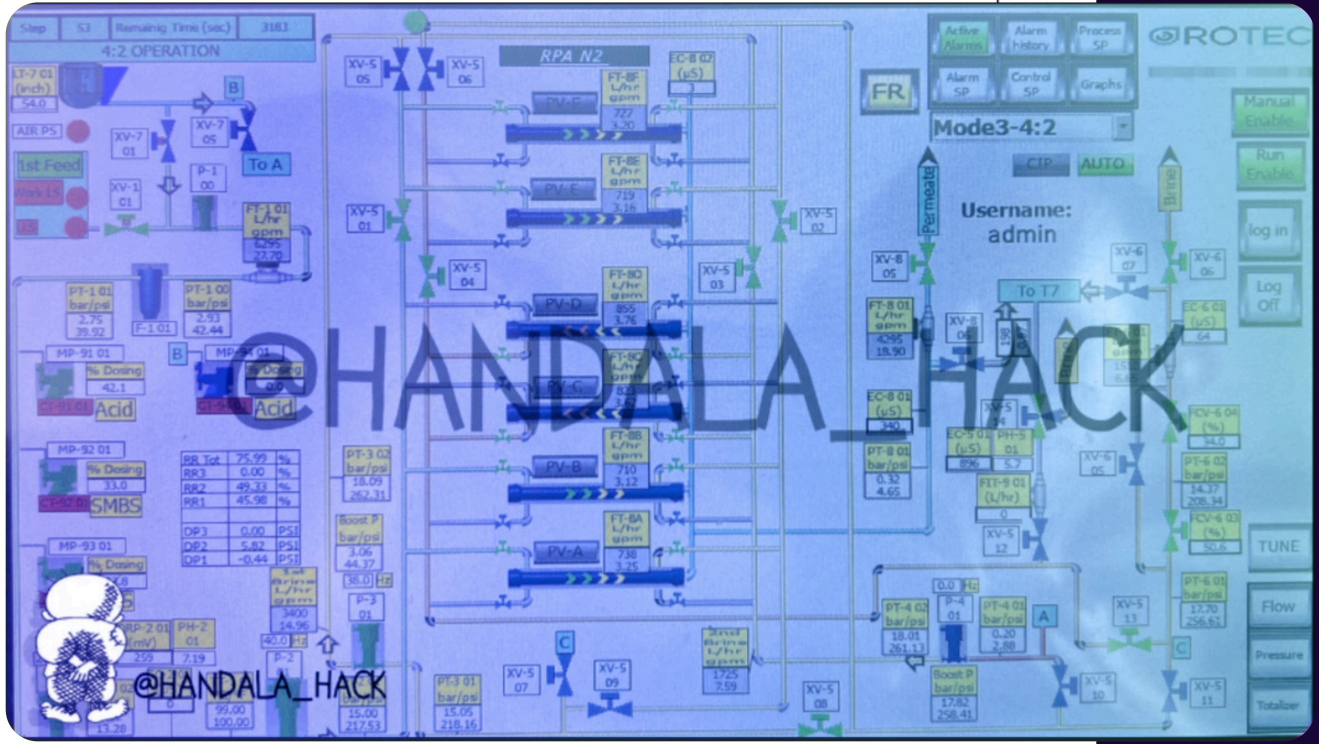
TARGETS_

Industry - OT

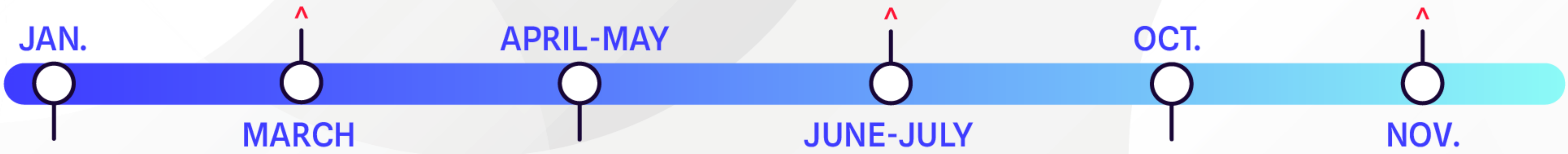
*2024: A turning point in targeting industrial infrastructure_*

The year 2024 also witnessed a significant increase in attacks targeting industrial infrastructure. While a rise in intensity had already been noticeable in previous years, the critical escalation for [OT (Operational Technology)]() began as early as January with the discovery of the FrostyGoop malware in Ukraine and the attack on water reservoir systems in Texas. These two incidents - one targeting heating systems in the dead of winter, and the other compromising water storage infrastructure- highlighted the deep integration of industrial systems into daily life and the potential consequences of malicious actions against them.

In the following months, other civilian-impacting industrial systems were also targeted. Notably, the pro-Palestinian group Handala_hack claimed responsibility for an attack on Israel's potable water desalination infrastructure. Although the group provided evidence of its activities, no official statements were issued to confirm its claims.



Screenshot of water desalination SCADA systems compromised by the Handala_hack actor



JAN.

Texas water facilities attacked

FrostyGoop targets Ukraine heating systems

MARCH

Failed attack on French hydroelectric infrastructure

Iranian hackers compromise Israeli nuclear facility IT network

APRIL-MAY

Potential Handalack attack on Israeli facilities (details unclear)

JUNE-JULY

Increased cyberattacks on Ukrainian defense sector

OCT.

Salt Typhoon campaign targets US telecoms

American Water Works breached

NOV.

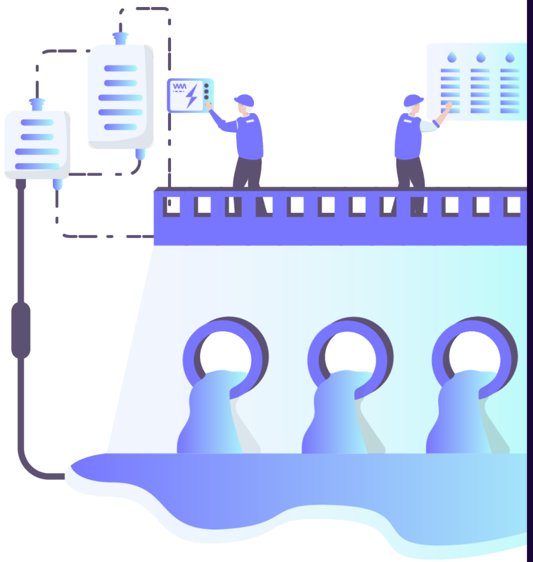
Iranian hackers target Israeli aerospace and defense industries

France was not spared from this wave of attacks. On March 2, 2024, an announcement from the Telegram group “Cyber Army of Russia Reborn” caught the attention of energy sector stakeholders. According to messages posted on the group’s Telegram channel, they claimed responsibility for an attack on the Courlon-sur-Yonne hydroelectric dam. Fortunately, the reality turned out to be far less dramatic: the actual target of the cyberattack was later identified as a watermill located in the village of Courlandon. Investigations revealed that the only impact was a 20-centimeter rise in water level, with no real consequences for residents.

Although attacks on water management infrastructure continued throughout the year, they were not the only incidents involving critical systems that generated significant media coverage. Other attacks targeting mobile telecommunications infrastructure had major repercussions, particularly the Salt Typhoon campaign.

The "Salt Typhoon" campaign was carried out by a suspected state-sponsored actor of Chinese origin and targeted American telecommunications systems, including Verizon, AT&T, and T-Mobile. The intrusion spread through roaming systems. Although it was discovered in October 2024, it likely began more than two years earlier.

Indeed, these networks are considered vital to national interests and are closely monitored by government authorities to prevent any disruption that could lead to the inoperability of emergency services. Because the primary focus is on availability, operators tend to concentrate their efforts on maintaining network uptime - explaining how such an attack could go unnoticed.



*The strategic value of industrial network sabotage_*

Among all the incidents mentioned during this period, three main types of attacks have been identified:

> Attacks on critical infrastructure systems (e.g., water distribution and hydroelectric power production)

> Attacks targeting essential civilian infrastructure in conflict contexts (such as FrostyGoop and the Handala_hack campaigns)

> Attacks on telecommunications systems aimed at spying on communications between third parties

These three types of attacks - carried out by state actors or hacktivists - highlight the emergence of new methods of warfare. In the cases of Handala_hack and FrostyGoop, the term “hybrid warfare” is appropriate, as cyber operations accompany actions in the physical world. These tactics, often unspoken and difficult to detect, have been used by certain countries for many years. What sets today’s operations apart is how widely they are communicated and shared.

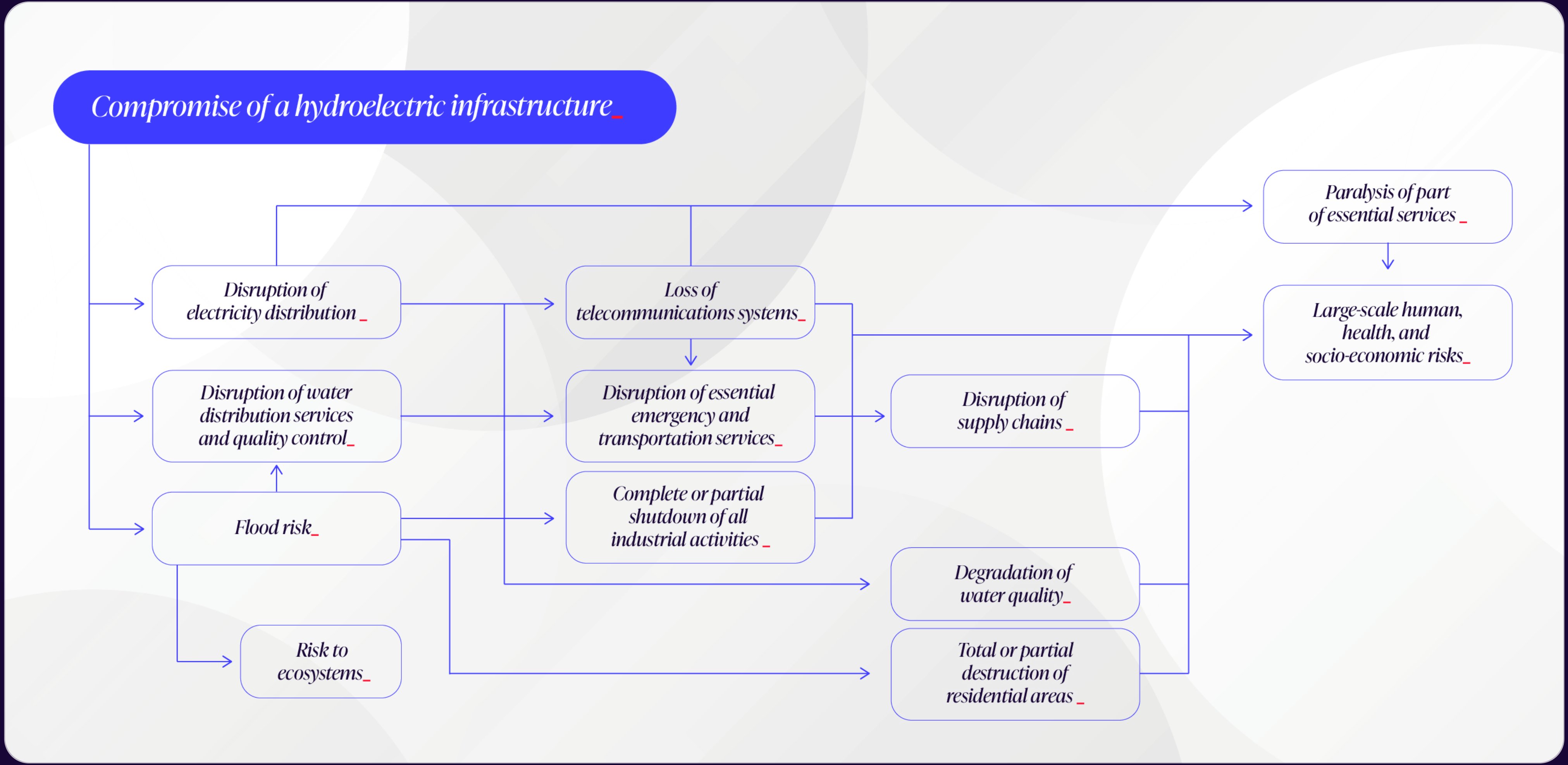
Nowadays, the widespread use of remotely controlled systems - whether for water networks or heating systems using poorly secured protocols - allows attackers to carry out actions that directly affect civilian populations. This kind of psychological pressure ensures a constant sense of danger, even hundreds of kilometers away from the front lines. Safety, in these circumstances, is an illusion.

The use of cyber weapons to apply continuous pressure on a state and its population can also serve as a form of retaliation. This was the intent behind the failed attack on the Courlon-sur-Yonne dam - not to target the main belligerents, but their allies.

*Potentially catastrophic consequences_*

The Courlon-sur-Yonne attack in March 2024, which targeted a hydroelectric power production facility and was claimed via the (now-defunct) Telegram channel of "Cyber Army of Russia Reborn", followed France's military support to Ukraine. Although the attackers struck the wrong target, the original malicious intent clearly demonstrated a desire to disrupt electricity production and potentially trigger a catastrophic situation.

Had the original target - a hydroelectric dam - been successfully compromised, the consequences could have been severe: beyond the impact on energy production, tampering with the management systems could have caused downstream flooding.



*Compromise of a hydroelectric infrastructure_*

*Disruption of electricity distribution_*

*Disruption of water distribution services and quality control_*

*Flood risk_*

*Risk to ecosystems_*

*Loss of telecommunications systems_*

*Disruption of essential emergency and transportation services_*

*Complete or partial shutdown of all industrial activities_*

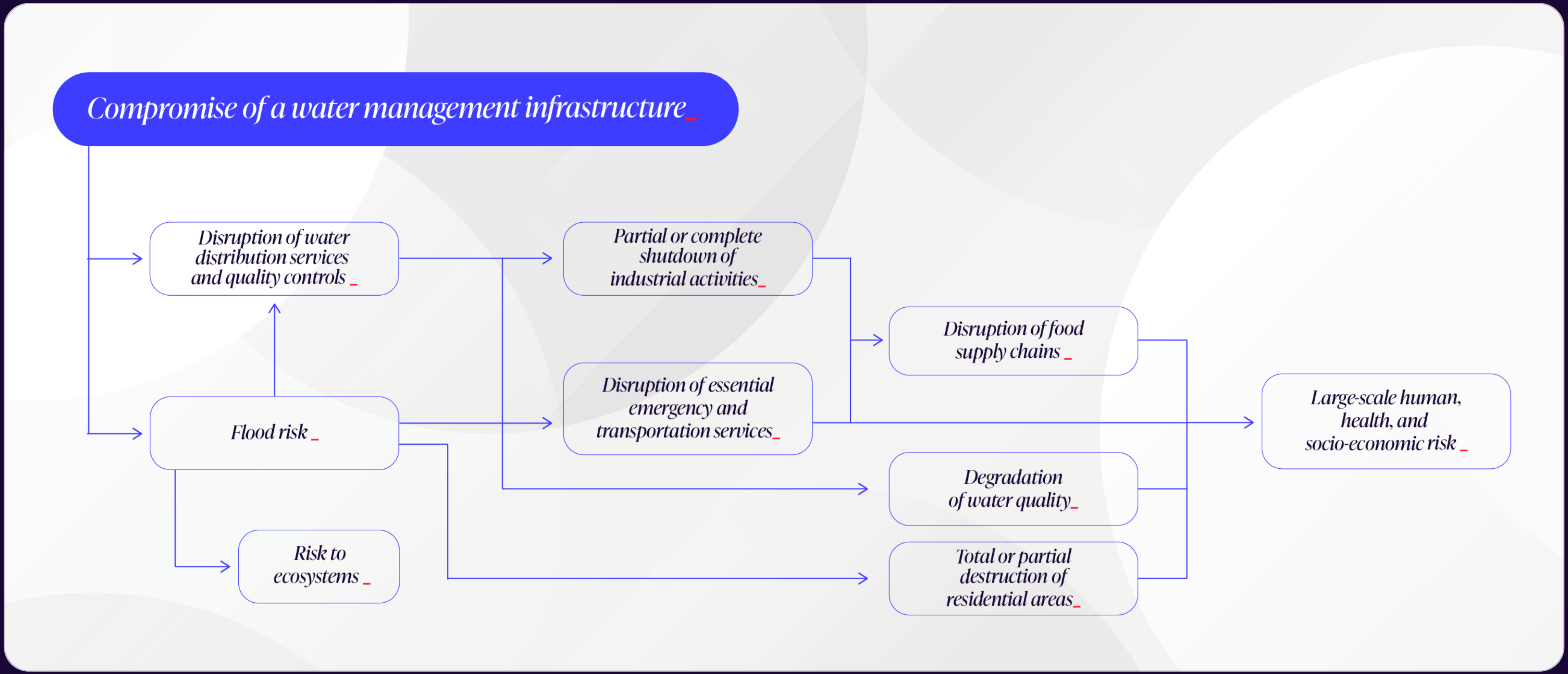
*Disruption of supply chains_*

*Degradation of water quality_*

*Total or partial destruction of residential areas_*

*Paralysis of part of essential services_*

*Large-scale human, health, and socio-economic risks_*



Compromise of a water management infrastructure_

Disruption of water distribution services and quality controls_

Flood risk_

Risk to ecosystems_

Partial or complete shutdown of industrial activities_

Disruption of essential emergency and transportation services_

Disruption of food supply chains_

Degradation of water quality_

Total or partial destruction of residential areas_

Large-scale human, health, and socio-economic risk_

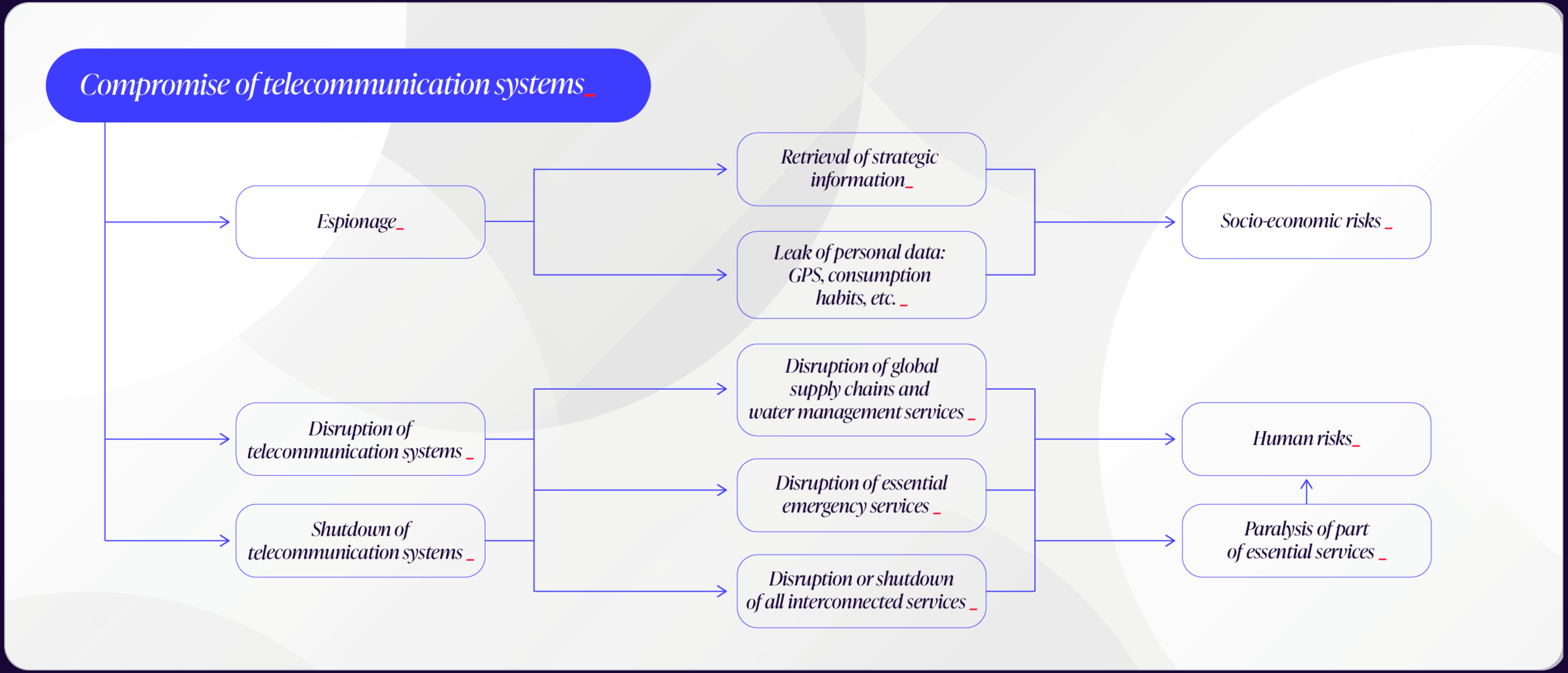
The same applies to attacks targeting water treatment and management systems in the United States. Although no group has claimed responsibility for these incidents, the intrusion and manipulation of automated systems can have catastrophic consequences.

If a malfunction occurs during one of the critical treatment phases - such as filtration, chlorination, or ozonation - or if wastewater and clean water come into contact, the resulting public health risks could be severe, potentially leading to loss of life.

*Large-scale espionage: The Salt Typhoon case_*

Salt Typhoon is a campaign carried out by a suspected state-sponsored Chinese-speaking threat actor that targeted U.S. telecommunications systems. At least nine companies were affected during this period, including major providers Verizon, AT&T, and T-Mobile.

This is not the first time Telecom Service Providers (TSPs) have been targeted in surveillance-focused cyberattacks.



*Compromise of telecommunication systems_*

*Espionage_*

*Disruption of telecommunication systems_*

*Shutdown of telecommunication systems_*

*Retrieval of strategic information_*

Leak of personal data: GPS, consumption habits, etc._

*Disruption of global supply chains and water management services_*

*Disruption of essential emergency services_*

*Disruption or shutdown of all interconnected services_*

*Socio-economic risks_*

*Human risks_*

*Paralysis of part of essential services_*

In 2020, the UNC1945 group had already targeted these same telecommunication systems for intelligence purposes. However, the modus operandi of these two actors is not the same. In the case of UNC1945, a list of IMSIs (mobile device identifiers) and MSISDNs (unique subscriber identifiers) was found in configuration files used to monitor a limited number of targets. In the Salt Typhoon campaign, however, the surveillance is much broader and could affect a large portion of the population.

The scale of these attacks is amplified by the interconnection services between telecom systems across countries, particularly through roaming networks.

While roaming allows seamless connectivity when traveling between countries, it also enabled the attackers to spread across systems. Although the campaign was discovered in October 2024, it is believed that the malicious activity had been ongoing for at least two years.

*A transformation in cyber threats_*

These events reflect an evolution in cyber threats - one that is not entirely new. What has changed, however, is the extent of media coverage, driven by advances in defensive capabilities.

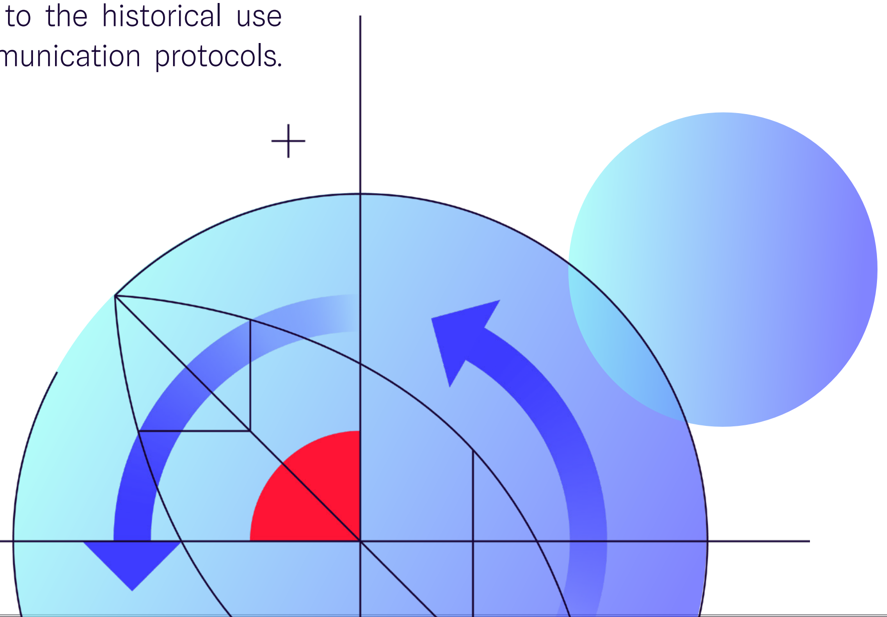
Indeed, the growing availability of security tools designed to monitor and supervise industrial systems has enabled the detection of attacks - and in some cases, active compromises - in environments that were previously overlooked by security teams.

Nevertheless, monitoring these systems remains a major challenge, primarily due to the historical use of outdated and insecure communication protocols.

Today, cyberattacks are an integral part of modern armed conflicts, offering attackers the ability to surgically strike their enemies and their allies alike.

It is critical to continue strengthening the security of these infrastructures, as attackers are becoming more skilled and are carrying out increasingly sophisticated attacks that impact the general public, leaving them in a constant state of insecurity.

To learn more (French): Secteur de l'eau : état de la menace informatique

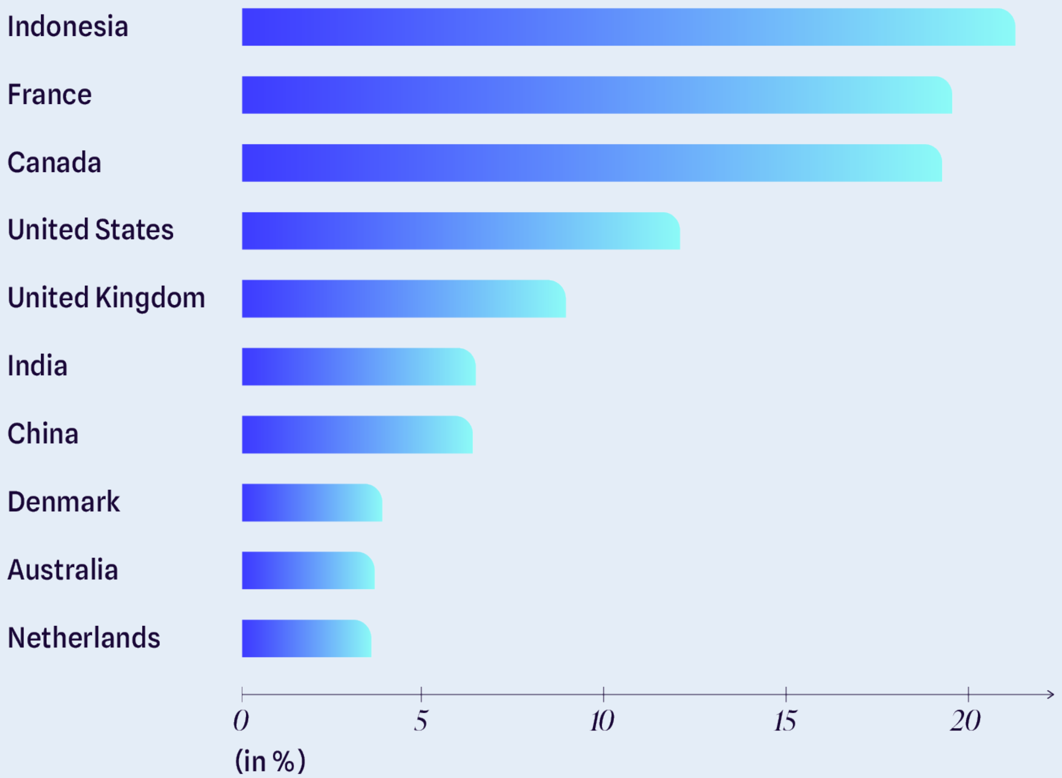


Paris 2024: A cyber challenge worthy of the games

The year 2024 placed France at the center of cyber threats, primarily due to the Paris Olympic Games. This global event drew the attention of APT groups, hacktivists, and cybercriminals, making French infrastructure a prime opportunistic target.

The ranking of the most targeted countries in 2024 confirms this, placing France in second position, just behind Indonesia.

TOP10 Most targeted countries in 2024



*The Olympics under high pressure_*

As early as 2023, ANSSI (France's national cybersecurity agency) warned of an unprecedented level of cyber risk, anticipating a significant surge in attacks during the Games. Even before the event began, scam campaigns targeted the public, with more than 300 fake ticketing websites identified[1].

At the same time, disinformation operations orchestrated by state-affiliated APT groups attempted to spread confusion, while industrial espionage efforts targeted the technological partners of the event[2].

Throughout the Olympic and Paralympic Games, cyber threats intensified, requiring heightened vigilance from authorities. According to ANSSI, 548 cybersecurity incidents were recorded, including 465 classified as low-impact and 83 considered more serious. Most of these attacks aimed to disrupt IT services, confirming cybercriminals' strong interest in the event. Thanks to extensive monitoring systems and protective measures deployed, no major incidents impacted the Games, demonstrating the effectiveness of the cybersecurity strategy in place[3].

Sources

[1] (FR) *20 Minutes*

[2] *Cloud Google*

[3] (FR) *cybergouv.fr*

*An unprecedented defensive framework_*

Aware of the cyber risks that had already impacted previous Olympic Games and other major international events, France implemented a reinforced cybersecurity strategy for Paris 2024. The digital infrastructure of the Games - spanning over 35 sites and involving thousands of devices - required an exceptional upgrade in protective measures.

Preparation relied on close coordination between public and private stakeholders, including technical partners such as Atos, Intel, Orange, and Cisco. Drawing on its experience from previous Olympic editions, Cisco ensured the security of the network and cloud infrastructure, while ANSSI (French National Cybersecurity Agency) played a central role by conducting security audits and leading simulation exercises to test the resilience of involved organizations. This approach also included increased awareness training for employees and service providers to reduce the risk of human error.

In addition, a proactive approach was adopted to identify and patch vulnerabilities before they could be exploited. For instance, SNCF Connect launched a **Bug Bounty** program on the YesWeHack platform, encouraging the cybersecurity research community to help uncover potential flaws. In parallel, a **Cyber Security Operations Center** (CSOC) was established to monitor and respond to threats in real time, leveraging **threat intelligence** and active monitoring of suspicious infrastructure.

Shortly before the event, Gatewatcher published an analysis detailing the challenges and countermeasures implemented to secure the Games' digital ecosystem[4]. Thanks to this forward-thinking strategy and the security measures deployed, France successfully minimized the impact of cyberattacks and ensured the smooth execution of the Games, setting a new benchmark for cybersecurity in future international events.

Sources

[4] *Gatewatcher.com*

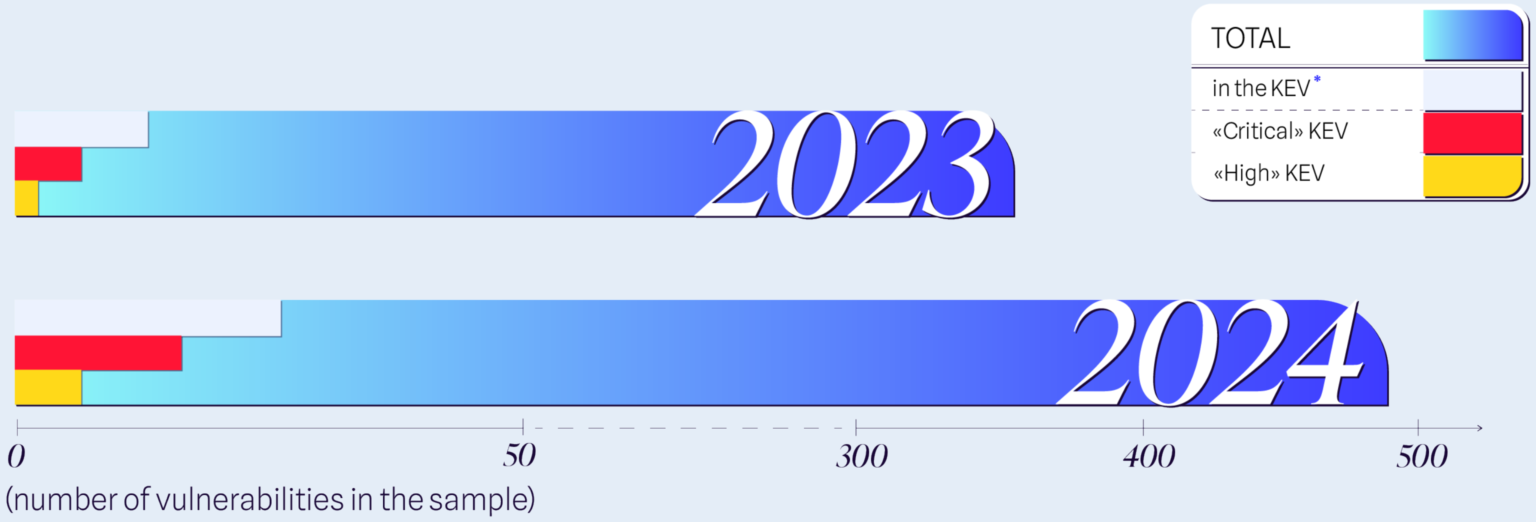
03

VULNERABILITIES: BETWEEN INNOVATIONS & PERSISTENCE_

Security in the crosshairs

The year 2024 was marked by the widespread exploitation of vulnerabilities, with 768 CVEs publicly reported as exploited - an increase of approximately 20% compared to 2023. This issue has placed the protection of information system assets at the core of corporate strategies. To address this, organizations are implementing various measures to restrict communications, ensure secure access to assets, and control the security settings of devices.

One key lesson from 2024: security solutions must be considered critical assets in their own right. As core components of a system's defense, they require dedicated attention to ensure operational readiness - through continuous monitoring, configuration management, and vulnerability oversight.



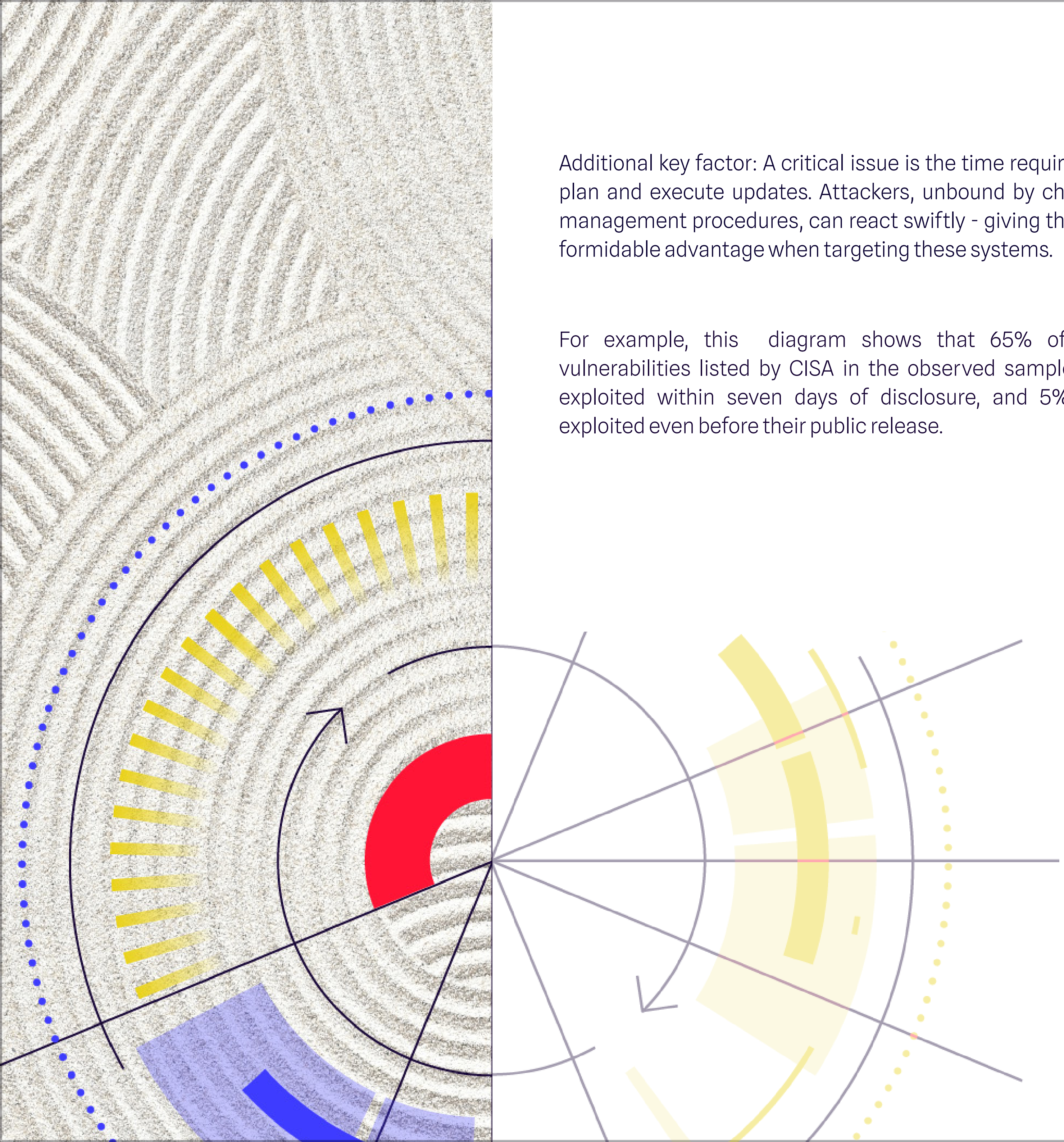
These devices, responsible for defending information systems, are becoming prime targets due to their strategic placement and the privileged access rights they often hold.

> The most striking example is the series of incidents affecting Ivanti, a U.S.-based cybersecurity company known for its VPN and endpoint management solutions. Over the course of the year, more than 180 vulnerabilities were reported in Ivanti products, including 26 that were actively exploited, despite significant internal security efforts.

Ivanti is not an isolated case. The number of vulnerabilities affecting a sample of five well-known security equipment vendors increased by 39% compared to the previous year. In total, the number of vulnerabilities observed in production environments rose by 66% in 2024.

Key insight from the graph: There has been a notable increase in the total number of vulnerabilities over the year, along with a sharp rise in exploited vulnerabilities, including those leveraged in ransomware attacks.

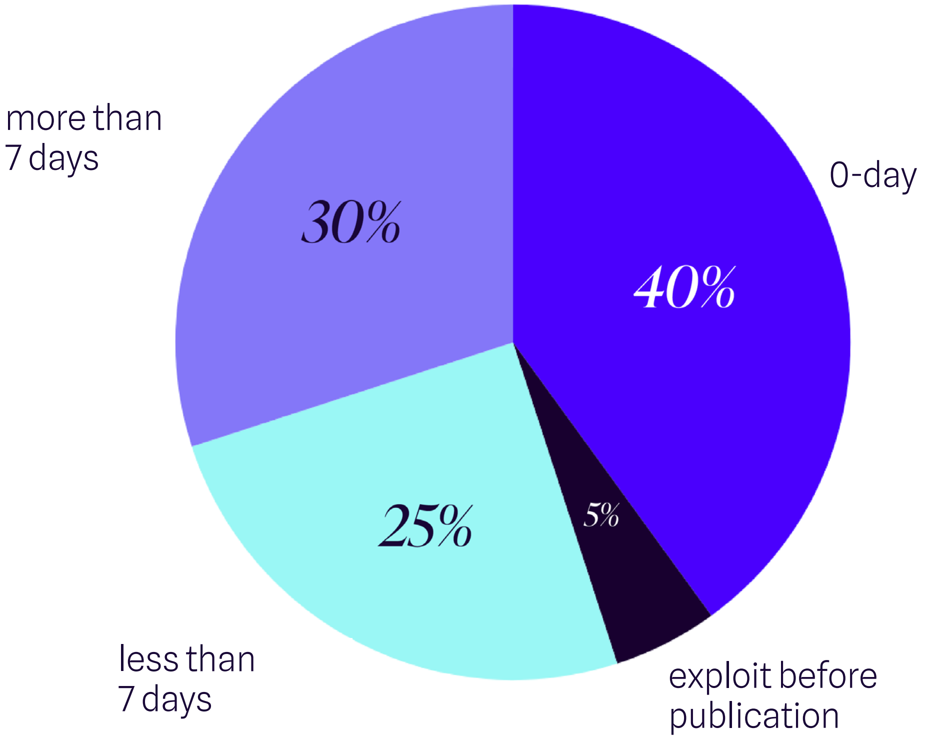
* *Known Exploited Vulnerabilities Catalog (KEV)*



Additional key factor: A critical issue is the time required to plan and execute updates. Attackers, unbound by change management procedures, can react swiftly - giving them a formidable advantage when targeting these systems.

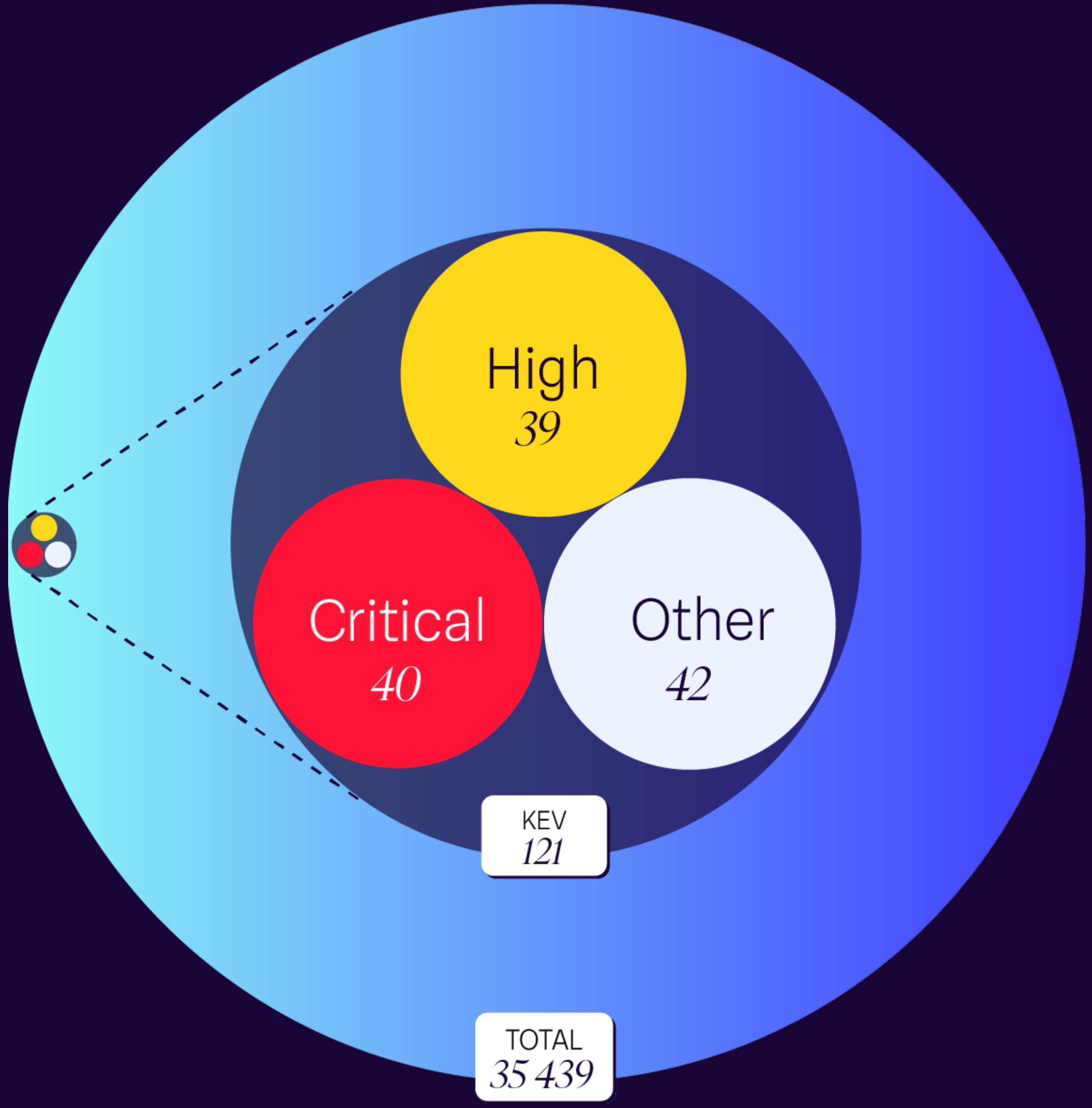
For example, this diagram shows that 65% of the vulnerabilities listed by CISA in the observed sample are exploited within seven days of disclosure, and 5% are exploited even before their public release.

*Time distribution between disclosure and exploitation of vulnerabilities in the sample_*



2024 Representation of exploited vulnerabilities_

The most exploited vulnerabilities represent only a small fraction of all published vulnerabilities. Among these, severity level is not always a determining factor. The **Known Exploited Vulnerabilities** (KEV) Catalog, maintained by CISA, helps security teams prioritize which vulnerabilities require immediate remediation. This catalog specifically lists vulnerabilities that are known to be actively exploited by threat actors.



*"Critical" vulnerability management_*

With a 21% increase in vulnerabilities between 2023 and 2024, organizations face a growing challenge in prioritizing patches and determining appropriate remediation timelines. For nearly two decades, the CVSS (Common Vulnerability Scoring System) has been used to assign a score out of 10 to vulnerabilities based on their severity. However, the Base Score Metrics - which focus solely on exploitation conditions and impact - are often used in isolation, without factoring in additional context such as threat or environmental modifiers.

The release of CVSS version 4.0 at the end of 2023 introduced a new labeling system that indicates whether threat or environmental modifiers are considered. Despite these improvements, the number of high-scoring vulnerabilities requiring action remains significant. In some cases, scores may be reassessed upward after further analysis or if vulnerabilities are combined with others. This underscores the importance of ongoing monitoring of threat actor activity, in order to respond quickly to vulnerabilities most likely to be exploited - using Cyber Threat Intelligence (CTI) tools.

In addition to reliable CTI, other resources such as alerts from various CERTs and the KEV Catalog can support better decision-making and vulnerability management.

Phishing 2024: Increased sophistication and rise of quishing

In 2024, phishing continued to gain momentum, with a 30% increase in attacks observed during the second half of the year. This growth can be attributed to the evolving techniques used by cybercriminals, who are now leveraging more sophisticated and harder-to-detect methods. While traditional email-based phishing remains widespread, new forms of phishing are emerging and gaining traction.

*Artificial Intelligence at the service of cybercriminals_*

The use of generative language models to craft more credible phishing campaigns had already been discussed in our 2023 H2 report. In 2024, this trend has been confirmed, with attacks becoming even more sophisticated—particularly due to the integration of artificial intelligence. AI now makes it possible to generate error-free, highly personalized emails that closely mimic legitimate communications.

This increased personalization makes spear-phishing campaigns even more effective, especially when targeting executives or employees with access to sensitive information.

More broadly, AI has also strengthened social engineering tactics, notably through the use of vocal and video **deepfakes**, which enhance the credibility of impersonation attempts and facilitate financial fraud or the disclosure of strategic information.

One incident highlights the scope of this threat: In early 2024, a multinational company fell victim to a scam involving AI-generated deepfakes during a video conference[1]. The scheme began with an email allegedly sent by the company's CFO based in the UK, requesting the execution of a confidential financial transaction. Initially skeptical, an employee from the Hong Kong subsidiary was reassured after attending an online meeting where AI-generated videos simulated the CFO and other colleagues.

Convinced of the request's authenticity, the employee initiated 15 wire transfers to multiple fraudulent accounts, totaling 25 million U.S. dollars, before the scam was eventually uncovered.

In response to these emerging threats, the FBI issued an alert[2] in late 2024, warning of the growing use of AI in cyberattacks.

Sources

[1] *scworld.com*

[2] *ic3.gov*

In April 2024, the MITRE ATT&CK® framework was updated with the addition of sub-technique T1588.007, titled "Artificial Intelligence"[1]. This update reflects the growing interest among cybercriminals in leveraging artificial intelligence. According to MITRE, such tools can be used for reconnaissance activities, the writing of basic scripts, supporting social engineering campaigns, and even developing malicious payloads.

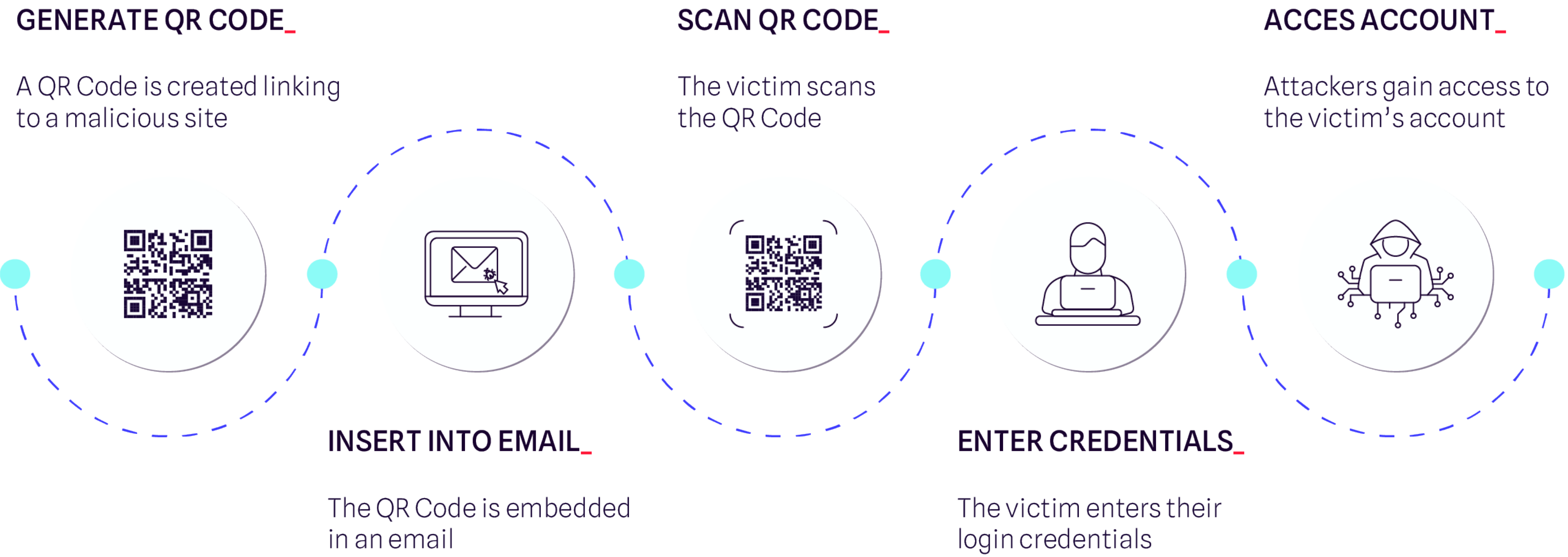
Sources:

[1] attack.mitre.org

*Quishing: A growing threat_*

While email phishing remains the most widespread technique, **Quishing**, —a more discreet and harder-to-detect variant, —experienced alarming growth in 2024. By taking advantage of users' trust in QR codes, this method allows cybercriminals to bypass traditional filters and more easily deceive their targets

*Cybersecurity Threat : QR Code Attack_*



GENERATE QR CODE_

A QR Code is created linking to a malicious site

INSERT INTO EMAIL_

The QR Code is embedded in an email

SCAN QR CODE_

The victim scans the QR Code

ENTER CREDENTIALS_

The victim enters their login credentials

ACCES ACCOUNT_

Attackers gain access to the victim's account

In February 2024, the UK's National Cyber Security Centre (NCSC) issued a warning about this threat in an article titled "QR Codes - what's the real risk?"[2], highlighting that attackers are increasingly using QR codes to hide malicious links in phishing emails, redirecting victims to fraudulent websites. The ENISA (European Union Agency for Cybersecurity) Threat Landscape 2024 also reported a significant surge in such attacks, confirming that cybercriminals are now widely using this technique to compromise access to cloud services and steal credentials[3].

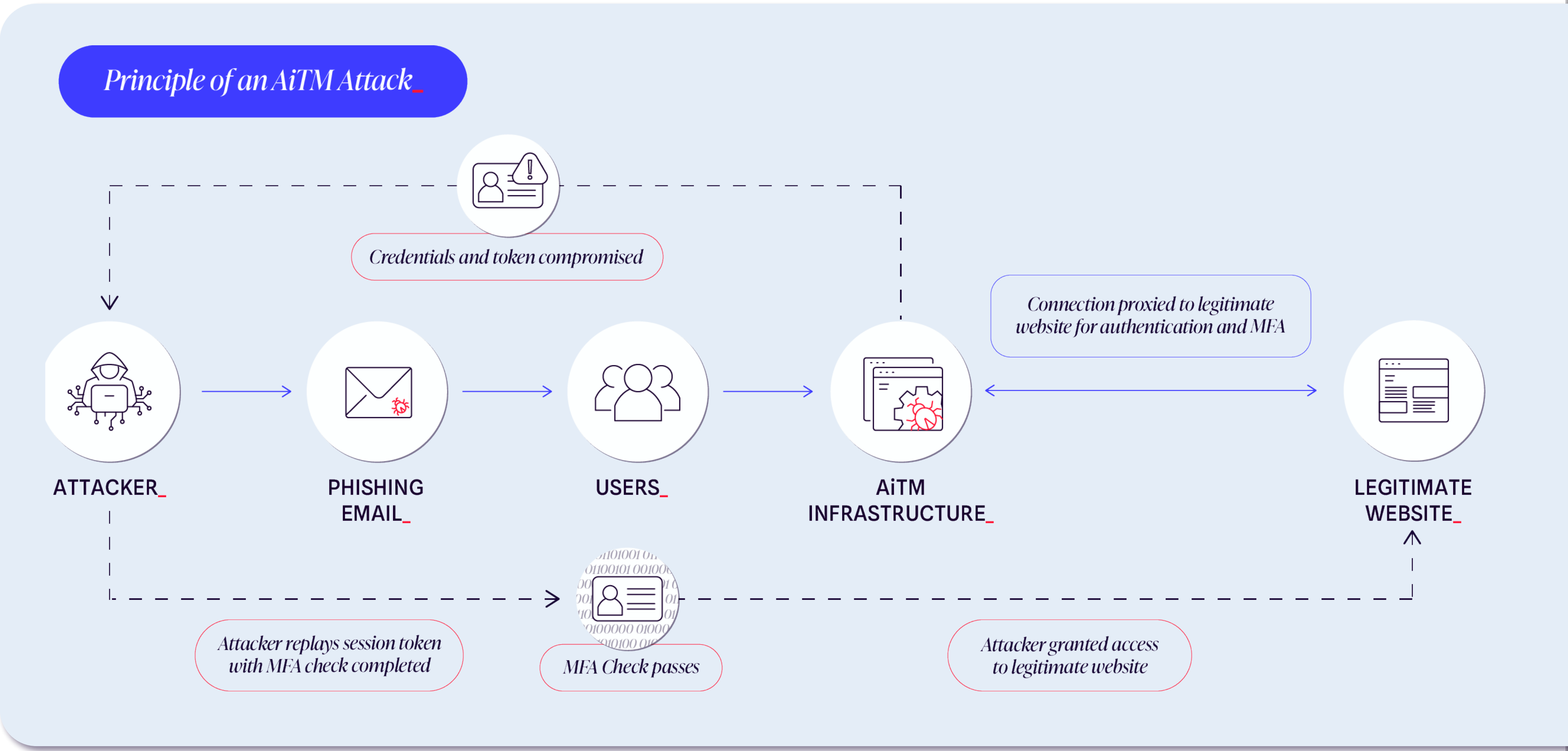
Sources:

[2] ncsc.gov.uk

[3] enisa.europa.eu

This trend became evident in July 2024 with a major attack exploiting Microsoft Sway[1]. Cybercriminals used the presentation-building platform to host malicious pages containing deceptive QR codes, prompting victims to scan them. Once scanned, the QR codes redirected users to fake Microsoft 365 login pages designed to harvest credentials and MFA codes. This campaign led to a 2,000% increase in traffic to phishing pages hosted on sway.cloud.microsoft, primarily targeting the technology, manufacturing, and financial sectors in Asia and North America.

The Quishing trend was also confirmed by an attack targeting cybersecurity firm Sophos in October 2024[2]. Cybercriminals leveraged Quishing to distribute fraudulent QR codes, tricking employees into scanning them under the pretense of following internal security procedures. Once scanned, the codes redirected to fake authentication portals designed to steal corporate account credentials. This campaign specifically targeted access to Sophos' internal applications, but its impact remained very limited thanks to the company's robust internal controls. While one employee was deceived and provided both their login credentials and multi-factor authentication (MFA) token, the attackers failed to access any sensitive internal data or assets.


*Principle of an AiTM Attack_*

Credentials and token compromised
Connection proxied to legitimate website for authentication and MFA
ATTACKER_
PHISHING EMAIL_
USERS_
AiTM INFRASTRUCTURE_
LEGITIMATE WEBSITE_
Attacker replays session token with MFA check completed
MFA Check passes
Attacker granted access to legitimate website

Notably, these attacks also rely on a well-known phishing technique: Adversary-in-the-Middle (AiTM). By inserting a malicious proxy between the victim and the legitimate website, cybercriminals can intercept not only login credentials, but also MFA tokens, enabling full account takeover and bypassing traditional protections.

The success of Quishing, which is increasingly becoming a go-to attack vector in modern phishing campaigns, can be attributed to several factors. First, QR codes bypass traditional security filters, which are not designed to analyze their content before scanning. Second, these attacks primarily target mobile devices, which are often less protected than corporate workstations. Finally, cybercriminals exploit the positive perception of QR codes, widely adopted for legitimate purposes, prompting victims to scan them without suspicion.

Sources:

[1] bleepingcomputer.com

[2] news.sophos.com

Conclusion_

While the past year confirmed the agility and resilience of cybercriminals, it also demonstrated that cybersecurity efforts are paying off. Every defensive advancement, every takedown operation, and every innovation in detection makes it increasingly difficult for adversaries to succeed. Yet, attackers continue to adapt—exploring new attack surfaces, exploiting unknown vulnerabilities, and refining their strategies to bypass established protections.

In 2024, cybercriminals evolved their approaches, relying on more flexible business models and increasingly sophisticated attack techniques. Stealers emerged as a favored tool for mass credential theft, while ransomware operations adopted more targeted and resilient strategies. At the same time, attacks on critical infrastructure and high-profile events revealed a growing intent to maximize financial, operational, and strategic impact. This constant adaptability highlights an environment where the speed and precision of attacks challenge traditional response capabilities.

In this context, a static cybersecurity posture is no longer sufficient. Organizations must move beyond reactive responses and embrace a dynamic approach, combining continuous monitoring, adaptive defenses, and anticipation of emerging threats. This means pushing the boundaries of detection and remediation, exploring new ways to analyze threat behaviors, and optimizing defensive capabilities at scale.

Gatewatcher's Purple Team remains committed to this mission: demystifying attacks, providing context to threats, and empowering organizations to regain the upper hand. Through this report, we hope to have offered you a clear perspective on the cyber threat landscape and valuable insights to help you better navigate future challenges. The evolution of threats is inevitable - but with a proactive and collaborative approach, it is possible to minimize their impact.

A publication by

PURPLE TEAM
GATEWATCHER

GLOSSARY_

*Infostealer (ou stealer)_*

> Malware designed to steal sensitive information such as login credentials and banking data.

*Commonwealth of Independent States (CIS)_*

> An intergovernmental organization composed of several former Soviet republics.

*Credential Stuffing_*

> An attack method using stolen credentials to access multiple accounts due to password reuse.

*Malware-as-a-Service (MaaS)_*

> A business model where cybercriminals rent or sell malware to other threat actors.

*Infrastructure Access Brokers (IAB)_*

> Cybercriminals who specialize in compromising and reselling access to IT infrastructure.

*Ransomware as a Service (RaaS)_*

> An illicit service in which ransomware developers lease their malware to other criminals.

*Operational Technology (OT)_*

> Hardware and software systems used to monitor and control industrial infrastructure.

*Telecom Service Providers (TSP)_*

> Companies providing telecommunications services, including internet and telephony.

*International Mobile Subscriber Identity (IMSI)_*

> A unique identifier assigned to a SIM card to authenticate on a mobile network.

*Mobile Station International Subscriber Directory Number (MSISDN)_*

> A unique identifier of a mobile subscriber within a network.

*Known Exploited Vulnerabilities Catalog (KEV)_*

> A database of vulnerabilities known to be actively exploited by threat actors.

*Deepfake_*

> Digitally manipulated media using AI to mimic faces or voices.

*Quishing_*

> A phishing technique that uses QR codes to redirect victims to fraudulent websites.

*Adversary-in-the-Middle (AiTM)_*

> An attack in which a cybercriminal intercepts and alters communication between two parties without their knowledge.

*Bug Bounty_*

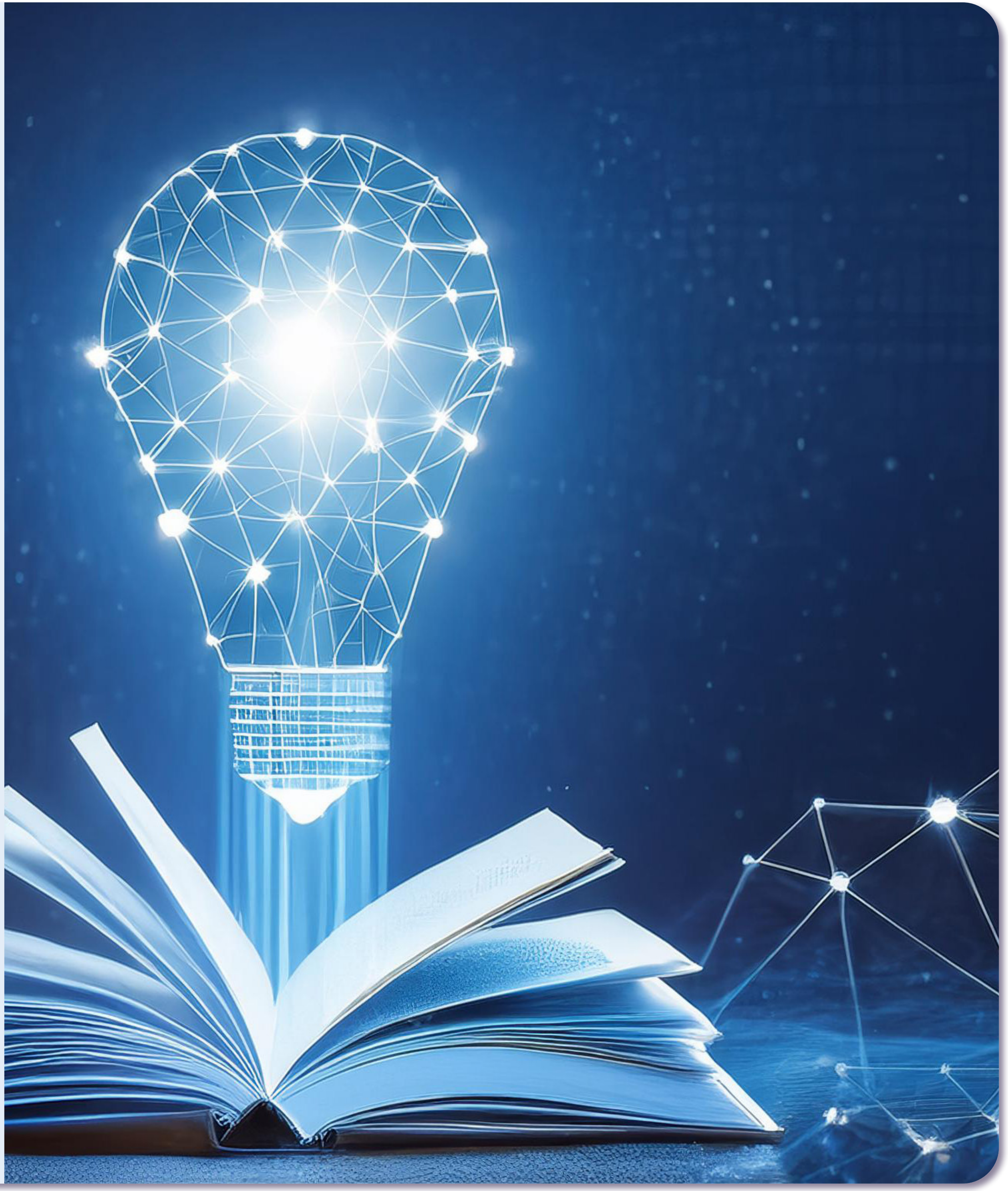
> A program encouraging cybersecurity researchers to find and report vulnerabilities in exchange for monetary rewards.

*Cyber Security Operations Center (CSOC)_*

> An operations hub that monitors, detects, and responds to cybersecurity incidents in real time to protect an organization’s digital infrastructure.

*Threat Intelligence_*

> The collection and analysis of data on cyber threats - including threat actors, tactics, and exploited vulnerabilities - to help anticipate and prevent attacks.



*Easy as_*

NDR_

CTI_

TAP_

GEN AI_

DEEP VISIBILITY_

About Gatewatcher_

A leader in cyber threat detection, Gatewatcher has been protecting the critical networks of major corporations and public institutions worldwide since 2015.

By combining AI with dynamic analysis techniques, we offer a 360°, real-time view of attacks across the entire network, in the cloud and on premise. Our Network Detection and Response (NDR) and Cyber Threat Intelligence (CTI) platforms enable us to characterize all types of threat as early as possible, in order to initiate global remediation actions. “Secured by design”, our qualified NDR meets regulatory requirements (PDIS, NIS 2, DORA, CRA) and guarantees enhanced detection of sensitive and off-line infrastructures.