CERT-IST

INDUSTRIE | SERVICES | TERTIAIRE

Cert-IST 2025 report on attacks and vulnerabilities in 2024

Released: February 2025

Contents

1 Introduction

Each year, Cert-IST publishes a report on the vulnerabilities, attacks and trends of the previous year to help the community protect itself more effectively.

The report begins with an analysis of key security events throughout the year (see § 2). We also offer a brief review of Cert-IST's activity during the year (§ 3).

In the conclusion (§ 4), we give a summary of the current cyberthreat landscape and the challenges companies will face in 2025.

➢ **About Cert-IST**

Cert-IST (Computer Emergency Response Team – Industry, Services and Tertiary) is a computer attack alert and response centre for businesses. Established in 1999, Cert-IST helps its members identify threats by continuously analysing new vulnerabilities, their severity and the protection measures needed. In the event of a security incident affecting one of its members, Cert-IST can assist with the investigation and the return to normal operations.

2 Analysis of the most significant phenomena in 2024

2.1 Three key events of the year

Here are our three most significant events of 2024.

2.1.1 Olympic and Paralympic Games

There's a general consensus that the Paris Olympic and Paralympic Games were a resounding success. This is also true from a cybersecurity perspective!

No major IT or cybersecurity failure caused any significant disruption to proceedings. The public will more likely remember the physical attacks just before the Opening Ceremony (sabotage of high-speed rail trackside equipment and internet cables) than the cyberattacks (mainly DDoS, but also ransomware attacks on the Grand Palais sports venue and museums), which did not cause any serious disruption.

This is a real achievement because attacks were expected. The specifics weren’t disclosed, but we can assume that more attacks took place and that the Olympics cyber response unit, ANSSI (France’s national cybersecurity agency) and the security teams from the various other stakeholders were involved in intensive behind-the-scenes work to prevent those attacks. A huge effort was made in terms of pre-event planning and real-time response to ensure this positive result.

On this occasion, France demonstrated its expertise in cybersecurity, confirming its already excellent reputation in this field. Everyone involved in this effort undoubtedly gained valuable hands-on experience, further improving their expertise and security posture. The next step is to build on these efforts and find ways to share this expertise as widely as possible.

2.1.2 CrowdStrike outage on 19 July 2024

On 19 July 2024, a faulty update to CrowdStrike’s Falcon EDR caused more than 8 million Windows systems worldwide to crash. This led to major disruption for organisations using the product, including airlines and hospitals.

The outage is reminiscent of similar incidents years ago (in the 2010s), when antivirus signature updates caused vital files on Windows systems to be mistakenly quarantined. Since then, the solution typically adopted has been to roll out updates in stages, starting with non-critical systems, to limit the scale of any incident should an update prove defective.

Following this incident in 2024, CrowdStrike strengthened its qualification procedures and Microsoft announced that it would make changes to Windows (and offer specific APIs) to protect the core of its operating system from direct updates by third-party products.

The staggered, risk-based rollout of updates (allowing companies to control how and when updates are applied to their systems) seems to us a vitally important preventive measure. We don’t know enough about the Falcon product to know if this is planned.

2.1.3 Attacks on edge devices

We observed this in 2023 and the situation was exactly the same in 2024: edge devices such as firewalls and VPN servers are under constant attack:

- They’re **too vulnerable** (in 2020 we described them as “tough on the outside, soft in the middle”). Many of the vulnerabilities exploited in 2024 were relatively simple, implying that products are older designs and not compliant with current best practice. The term “unforgivable vulnerability” became a buzzword in 2024.
- They’re **difficult to monitor** (no EDR).
- They’re **difficult to disinfect** because the attacker infiltrates deep into the underlying platform (often a Linux or FreeBSD system).

Here are the nine most significant attacks of this type in 2024 (there were seven in 2023):

- **Ivanti** Connect Secure CVE-2023-46805 (January)
- **Fortinet** VPN SSL CVE-2024-21762 (February)

- **Cisco** ArcaneDoor CVE-2024-20359 (April)
- **Palo Alto Networks** GlobalProtect gateway CVE-2024-3400 (April)
- **Check Point** VPN CVE-2024-24919 (May)
- **SonicWall** CVE-2024-40766 (August)
- **Ivanti** Cloud Services Appliance CVE-2024-8963 (October)
- **Fortinet** FortiManager CVE-2024-47575 (October)
- **Palo Alto Networks** CVE-2024-0012 (November)

These attacks show that:

- **Memory-only infections have become the norm** for advanced attackers. More specifically, this type of attack is simple and precise: the hacker installs a minimal piece of malware in the system's memory (in an existing process). This malware then executes whatever commands (or additional binary modules) are sent to it. This is true for state-sponsored attacks (e.g. ArcaneDoor on Cisco), but also for some cybercriminal attacks.
- **Attackers exploit less-monitored devices.** Paradoxically, these include firewalls and security appliances, which are non-EDR devices with few internal monitoring mechanisms (i.e. few logs about device operation). Also in 2024 we saw attackers gaining access to poorly secured Big IP equipment. Connected (IoT) devices in the corporate environment could also be easily targeted.
- **Linux/Unix malware is on the rise.** Most likely, this is simply the effect of the previous point, since many security appliances run on Linux/Unix. However, this doesn't imply there were fewer attacks infecting Windows devices.

The relentless attacks on edge devices create crisis situations and increasing fatigue for operations and security teams. In 2024, this led to a backlash and demands for change from software vendors. We discuss this point in § 2.6.

2.2 The actors behind the attacks

In 2024, state-sponsored attacks attracted most of our attention, and we discuss them in §2.3. But, of course, all the other actors were no less active. In this section, we review each of them in turn.

2.2.1 States

2.2.1.1 Sophisticated and discreet attacks

State-sponsored attacks take many forms, but they differ from other types of attacks because:

- Attackers are capable of a high level of sophistication.
- They're often discreet and deep, with the goal of remaining inside the target organisation for a long time (known as a pre-positioning attack).

The **Big Four** most-cited states in our reports remain unchanged: China, Russia, North Korea and Iran.

Several commentators noted in 2024 (for example, see here) that little is said about attacks by all the *other states*, especially the offensive cyber operations by Western countries. The reasons cited are that (a) these attacks are likely more discreet, and (b) it could generate conflicts of interest (it might be problematic for a French company to publish information about a French state-sponsored attack).

2.2.1.2 Disinformation and Info Ops: an integral part of the offensive trilogy

2024 confirmed a trend that emerged in 2016 (with Russia's influence operation on the US elections): malign information operations (or **Info Ops**, also known as **FIMI** in Europe) are **increasingly common**, and nations must now actively defend against these types of cyber and information warfare attacks.

For several years now, Russia has been the country most cited for its offensive operations in this domain. **Iran, China and Azerbaijan were also active in 2024.**

Offensive capabilities of states

- From an offensive perspective, we generally observe three types of offensive capabilities used by states: cyberattacks (DoS, sabotage, etc.), cyberespionage and influence operations (information warfare).

- In France, national defence strategy defines three domains of cyber warfare: *Lutte Informatique Défensive* (LID, or defensive cyber warfare), *Lutte Informatique Offensive* (LIO, offensive cyber warfare) and *Lutte Informatique d'Influence* (L2I, cyber influence warfare).

2.2.2 Cybercrime

2.2.2.1 Short-lived attacks driven by financial gain

Cybercriminals are primarily interested in making money. Unlike state-sponsored attackers, they aren't really interested in discretion or long-term operations, since the most common tactic for a hacker group is to dissolve if it becomes too visible, then re-emerge in another form.

The main areas of activity are scams, fraud (bank fraud, BEC attacks, fraudulent wire transfer requests, etc.) and ransomware, which has been the dominant form since 2019. Cryptocurrency theft has also been an extremely active field for several years, but with specific targets (cryptoasset holders and trading platforms).

Since 2022, infostealers have become a widespread phenomenon, which continued in 2024 with no significant change.

Note: ransomware is now used to describe attacks that encrypt company data, as well as attacks in which the attacker simply steals the data (data exfiltration) and then threatens to disclose it.

2.2.2.2 What's new in ransomware?

Ransomware attacks are still on the rise, but we've seen a **linear increase** in the last two years **rather than exponential increase** (as was the case in 2020 and 2021). In 2024, between 300 and 400 new victims were reported each month.

Large ransomware groups tend to disappear, often as a result of legal action against them (see below), but other, smaller groups appear all the time. It's almost as if enforcement operations against a large group simply fragment it into a series of smaller groups.

Groups in decline in 2024: **LockBit 3.0** (virtually ceased activity since August 2024, but announced a comeback in late 2024 with LockBit 4.0), **Cl0p** (very little activity in 2024 until its comeback in late 2024 with the Cleo attack) and **ALPHV/BlackCat** (self-dissolved in March 2024).

Groups gaining prominence include: **RansomHub**, cited by all analysts as the most prominent group in 2024. Other groups such as **PLAY**, **Medusa** and **Akira** are also mentioned by some analysts.

2.2.2.3 Unprecedented number of arrests and takedowns

The fight against ransomware, and malware in general, began to intensify from May 2021 in response to the Colonial Pipeline attack. This phenomenon has continued to grow, and **2024 was a record year on this front** (SOCRadar provides a list of 32 major law enforcement operations in 2024).

We would highlight in particular:

- **Operation Cronos** (February) against LockBit.
- **Operation Endgame** (May) against Loaders IcedID, Pikabot, Trickbot, Bumblebee, Smokeloader and SystemBC.
- Arrest of the hacker known as **USDoD** in Brazil (October).

- **Operation Serengeti** (November): arrest of over 1,000 cybercriminals in Africa (action coordinated by Interpol and Afripol).
- **Operation Passionflower** (December) with takedown of the MATRIX encrypted messaging system in Europe (coordinated by Europol and Eurojust).
- **Operation PowerOFF** (December) against 27 DDoS services (joint operation involving 15 countries).

2.2.2.4 New trend: Phishing-as-a-Service (PhaaS)

Phishing-as-a-Service first appeared in 2022 (with tools like Caffeine and EvilProxy) and made significant advances in 2024 with tools like **Tycoon2FA**, **Rockstar 2FA** and **SniperDZ**.

PhaaS are paid websites (SaaS services) that offer a set of tools for carrying out a phishing campaign: design of phishing emails, email distribution and password capture through fake login webpages. They’re reputed to be able to bypass 2FA authentication, since they implement AiTM attacks (Adversary-in-the-Middle, a technique where the victim connects to a fake website which relays traffic to the legitimate site). This attack works on simple MFA systems (SMS or OTP), but not on more advanced systems (known as phishing-resistant) that use mutual authentication.

2.2.3 Hacktivism

2.2.3.1 Often manipulated by state-sponsored hackers

Hacktivists were much in the news in 2024, especially with DDoS attacks (typically the pro-Russian attacks by the **NoName057** group) and also with Hack&Leak and even destructive attacks (Ransomware, Wiper). We haven't noted any significant changes in the techniques they use from 2023.

The vast majority of these attacks are linked to armed conflicts: Russia's war against Ukraine (since 2022) and the conflict between Hamas and Israel (since October 2023). These hacktivist movements are encouraged by states (for example, the Cyber Army of Ukraine was formed in 2022 by the Ukrainian government).

Creating or influencing hacktivist groups is undoubtedly one of the methods states can utilise for offensive cyber actions (just like organising Info Ops-type actions).

2.2.3.2 Low visibility for conventional hacktivist groups (lost in the crowd)

Apart from hacktivist actions linked to armed conflict, little was seen of other (conventional) hacktivist groups in 2024, and they had no significant effect. One example is the Operation Free Durov action launched after Telegram CEO Pavel Durov was detained in France. It was a DDoS attack campaign that lasted several days, but didn't really stand out from the pro-Russian DDoS attacks carried out by NoName057 at the same time.

2.2.4 Blurred boundaries between these groups

It can sometimes be difficult to draw a clear line between the actions of the various categories of hackers:

- States (especially Russia) seek to control or influence the actions of cybercriminal or hacktivist groups.
- Some states (notably North Korea and Iran) carry out attacks for financial gain (like cybercriminals).

A fourth category is often added to the other three: **Hackers for Hire**. They work either for cybercriminals (offering their services to anyone willing to pay), or for governments (carrying out specifically tailored attacks on demand).

2.3 Focus on the state-sponsored threat

Here are a few of the state-sponsored attacks in 2024, which demonstrate the level of sophistication these hackers can achieve.

2.3.1 *Russian APT29 group compromises Microsoft's corporate email system*

In January 2024, Microsoft announced that its Exchange Online corporate mail system had been compromised in November 2023 by the Russian APT29 group. This group (also known as Midnight Blizzard or Nobelium) is part of Russia's foreign intelligence service, or SVR, and is considered the most technically advanced group in Russia.

This attack enabled APT29 to steal access codes from several Microsoft customers, including US government agencies.

The attack technique used was remarkably sophisticated and shows that the hacker had perfect mastery of the Azure Cloud environment, authentication mechanisms and associated access rights:

- The hacker entered a test tenant, thanks to an account with a weak password.
- In this environment, they found a test app that had been approved by a privileged user in the Microsoft production environment.
- By utilising this approved app, they were able to act on the production environment and trigger a series of actions leading to the acquisition of access rights on all Exchange mailboxes.

Note: our summary above is brief, but it clearly shows the complexity of the attack and how it required a perfect knowledge of authentication mechanisms and privileges assigned to apps in order to be implemented. SpecterOps and Wiz.io provide a fuller insight.

2.3.2 *I-Soon, Pacific Rim and China's offensive cyber ecosystem*

As in 2023, China was omnipresent in 2024 for state-sponsored attacks, mainly **Volt Typhoon** (attack against critical infrastructure in the US) and **Salt Typhoon** (compromise of nine telecom operators in the US), but also **Flax Typhoon** and **Silk Typhoon**.

[Taxonomy]

Most of these Chinese groups had previously been identified but under separate names. Microsoft's new 2023 threat naming system grouped them into a single threat family called Typhoon. This change further reinforces the perception that China's cyber influence is pervasive and far-reaching. CrowdStrike uses the name Panda (since 2015) but it is now less common than Typhoon.

Beyond these attacks, several publications in 2024 showed how the Chinese state has structured its cyber-offensive activity. Here are the main ones.

I-Soon data leak. In February 2024, an unknown individual posted on GitHub documents stolen from the Chinese company I-Soon. They show that this company works mainly for the Chinese government. I-Soon provides intrusion and espionage services and promotes its ability to analyse and summarise stolen documents. It isn't believed to have advanced attack capabilities but relies on basic attacks using phishing. The I-Soon documents also show that the Chinese government distributes zero-day exploits discovered during national competitions like the Tianfu Cup to a range of Chinese companies engaged in offensive cyber operations.

Chinese ORB botnets. There was a lot of discussion in 2024 about these botnets deployed by China. Each botnet node is an ORB (operational relay box), i.e. a compromised machine used to mask the attacker. **KV-Botnet** (seen in Volt Typhoon attacks), **ORBWEAVER** and **Raptor Train** (seen in Flax Typhoon attacks) are three examples of Chinese ORB botnets revealed in 2024. This type of botnet has also been deployed by other countries. In 2014, after the Snowden affair, there was talk of similar projects: **HACIENDA** (UK) and **LANDMARK** (Canada). In 2018, the Russian **VPNFilter** botnet (set up to attack Ukraine) was discovered.

Sophos Pacific Rim. In October 2024, Sophos published a series of articles entitled Pacific Rim, which describe five years of attacks (from 2018 to 2023) by Chinese state actors against Sophos firewalls. This publication shows in particular how the offensive ecosystem is organised:

- The zero-day exploits against Sophos firewalls were developed at a Chinese university (the University of Electronic Science and Technology of China in Chengdu, Sichuan Province).
- They were then used by several Chinese groups (Volt Typhoon, APT31 and APT41/Winnti).

2.3.3 Nine US telecom operators compromised by Chinese Salt Typhoon group

In October 2024, it was announced that the Chinese **Salt Typhoon** group had successfully infiltrated the internal networks of several telecommunications operators in the United States and in particular AT&T, Verizon and Lumen. According to official statements, the attackers are believed to have:

- Gained access to data relating to legal wiretapping of communications (this made the attacker aware of who had been placed under surveillance by the US government).
- Wiretapped the communications of a limited number of people (political figures).
- Stolen customer call records/metadata.

The attack is believed to have lasted a year or more and was due (at least in part) to inadequate measures by these operators to protect their infrastructure.

It was one of the most significant attacks of 2024 and received a lot of media coverage.

2.4 Cloud attacks

2.4.1 *SaaS, IaaS, M365 and on-premise: a complex architecture*

For companies today, the cloud is generally made up of three parts, each with its own specific security weaknesses:

- **SaaS:** this includes all SaaS services used by the company, such as ServiceNow and SalesForce. This is undoubtedly the easiest component to manage in terms of security, since it's the SaaS provider who's responsible for maintaining the solution's security level. However, the user company generally has very little visibility into the security events that occur there (no supervision).

- **IaaS:** this includes all the company's applications deployed in Azure, AWS and Google Cloud. Here we find more or less the same problems of maintaining security levels as with on-premise applications. The most common type of attack is exploitation of a vulnerability.

- **M365:** this is the office and collaboration environment. The main difficulty here is managing identities and access rights. Account theft (phishing) is the most common type of attack.

In addition to these cloud components, companies also have on-premise services, which are either legacy applications or designed to meet specific needs. These services may also need to interact with the cloud infrastructure.

2.4.2 *Increasingly competent hackers*

The number of attacks on cloud infrastructure is increasing. We don't have exact figures on this phenomenon, but we observe it via the reports we analyse as part of our Attack and IoC monitoring service. This increase is quite logical, because more and more businesses are migrating their information systems to the cloud.

CrowdStrike provides some insightful figures on this subject in its 2024 Global Threat Report (dealing with incidents in 2023):

- It indicates a **75% increase** in intrusions into cloud environments.
- In most cases, the attacker doesn't even know they're in the cloud (they've remotely exploited a vulnerability and compromised a machine, which happens to be hosted in the cloud). They haven't attempted an attack on the cloud environment itself.
- But a growing number of hackers are aware they're in the cloud and are trying to exploit its specific features. They can, for example, gain privileges to access other cloud resources and create their own VMs. The number of this type of attacker, which CrowdStrike describes as **cloud-conscious**, is **up 110%** on the previous year, while cloud-agnostics (the previous category) are up 60%.

Note: 2023 (covered in the CrowdStrike report) seems to us a pivotal year. We observed highly agile hackers in cloud environments (such as Scattered Spider) carrying out spectacular attacks, which are now referred to as "cross-domain". This is where an attack starts on a compromised Windows workstation (domain 1), propagates to a Linux server in the cloud (domain 2) and then manages to gain a foothold in the cloud's management layer (domain 3), and so on.

2.5 Supply chain attacks

Since at least 2020 (and the SolarWinds attack via a compromised update), the threat posed by supply chain attacks has been well known. They can take many forms, but **attacks on the software supply chain** are the most frequent. In 2024, we once again saw multiple cases where software libraries made available on the internet had been compromised with malware. These are usually NPM packages (JavaScript packages for Node.js).

Below we describe the three examples of supply chain attacks in 2024 which we deem most relevant. The first two are in the category of software supply chain attacks.

2.5.1 XZ Utils attack

This attack is considered one of the most significant of 2024.

In late March, it was discovered that an attacker called **Jia Tan** (probably a pseudonym) had compromised the **XZ Utils open-source project** (which provides the liblzma compression library used by many software applications) with the aim of introducing a backdoor into the OpenSSH server on a large number of Linux systems. This attack is remarkable because:

- It targeted OpenSSH in an indirect way (via a library).
- It was a long and discreet effort: Jia Tan began contributing to the XZ Utils project in 2021, initially in a minimal role, then gradually introduced his backdoor into the library build and development process.
- The backdoor was sophisticated and the OPSEC (security measures taken to ensure no traces lead back to the attacker) was meticulous.

All these factors point to a campaign by a highly advanced hacker group. Unfortunately for them (and fortunately for us!), after almost three years of effort (from 2021 to 2024), the backdoor was discovered just 20 days after the last piece enabling it to be activated had been introduced into the project. Software developer **Andres Freund** found it when he noticed his OpenSSH server was generating too much CPU usage.

This example shows both the weakness of open-source software (which can be compromised by malicious contributors) **and its strength**, because when a savvy programmer examined the code he quickly uncovered the malware.

2.5.2 Polyfill.io attack

Polyfill.js is a popular JavaScript library used by about 4% of all websites. It's distributed by several sources, but many websites use the cdn[.]polyfill[.]io distribution site.

In February 2024, Chinese company Funnull acquired the polyfill[.]io domain. In June, researchers realised that the Polyfill.js library distributed by this domain was now malicious (redirecting to ad sites and injecting malware into mobile phones).

All websites that directly referenced cdn[.]polyfill[.]io then started distributing malicious content to their own visitors.

This incident illustrates a kind of supply chain attack that (to our knowledge) hadn't been seen before.

2.5.3 SaaS attacks on Snowflake and BlueYonder

These two attacks targeted SaaS solutions, which is new in the cyberthreat landscape.

Snowflake.com, which offers cloud-based data storage and analysis services, suffered a series of attacks targeting its customers. In May 2024, data belonging to **TicketMaster** (event ticket sales) and **Santander** (Spanish bank) were stolen from Snowflake. Analysis published by Mandiant shows that over 165 Snowflake customers were affected. Then in July, **AT&T** announced it was one of the victims. It was initially suspected that Snowflake was responsible for the breach (an employee account hacked and vulnerabilities exploited), but this was refuted by Mandiant, which analysed the incident. In fact, customer accounts had been stolen (via infostealers, then posted on underground marketplaces) and used to access their data stored at Snowflake. Mandiant reported that some of the victims were subcontractors which managed several customers (compromising a subcontractor enables attackers to steal the Snowflake accounts of all its customers). The attackers were identified and arrested later in the year.

BlueYonder.com, which offers cloud services to manage and optimise the supply chain (manufacturing, shipping and points of sale), suffered a ransomware attack in November that made its SaaS service unavailable to several customers such as **Starbucks** in the US, supermarket chains in the UK (**Morrisons** and **Sainsbury's**) and **BIC** in France. The attack was attributed to the Termite group and could be linked to the Cleo attacks claimed by the ClOp group at the end of 2024 (but this is denied by BlueYonder).

SaaS services are an attractive target for cybercriminals, because they can put pressure on both customers and the cloud solution provider. After the two attacks in 2024, this type of attack will likely increase in the years ahead.

2.6 Vendors need to be legally liable

The growing trend of security breaches affecting edge devices in 2024 (see § 2.1.3) has led to dissatisfaction among companies using these products. This includes the teams managing these devices (who all too often have to apply urgent new patches) and the CERT teams responsible for the company's security.

This frustration is part of an older and broader protest (not limited to vulnerabilities in edge devices) against the endless stream of patches released by vendors. Faced with such "patch fatigue", operational system managers are asking vendors for higher quality (reliability) in the software they sell.

In 2024, these issues were discussed at length by CERTs. Government bodies also seem to share these concerns: Europe has been working on a regulatory framework for several years, and the US, with a completely different approach, has launched CISA's Secure By Design initiative.

We discuss these issues in more detail below.

2.6.1 Gradual strengthening of Europe's legal framework

Here's what we said in the lead article of our Cert-IST monthly bulletin in October 2024.

> More and more voices are calling for binding legal liability on suppliers regarding the reliability (and especially security) of their software and hardware solutions.
>
> For example, the professional association InterCERT France (in which Cert-IST plays an active role) published a press release and an article on this topic in October. Based on the multiple vulnerabilities that have recently affected some security appliances (Ivanti ICS might come in mind), the association calls for new laws to hold software publishers liable. It also suggests 2 other directions (as an alternative to use weak products): use qualified products or, in some cases, use open-source solutions.
>
> Other initiatives are also moving in this direction. For example, at European level:
>
> - The obligation to report 'significant' vulnerabilities to French ANSSI (this obligation results from the French military programming law), published in May 2024, which requires manufacturers to report the most serious vulnerabilities and incidents to the ANSSI (French National Agency for Cybersecurity).
> - The Council of Europe directive published in October 2024, which proposes to include software and hardware in existing consumer protection laws (legal liability in case of defective product).
> - The European CRA (EU Cyber Resilience Act) regulation, which should come into force in 2027, and which aims to balance responsibilities between suppliers and end users.
>
> As this analysis (entitled 'The EU Throws a Hand Grenade on Software Liability') shows, Europe is more active than the USA in this area.
>
> It is worth noting, however, that in October 2024, the US SEC sentenced Unisys, Avaya, Check Point and Mimecast for downplaying the scale of the intrusions they suffered in 2020 during the SolarWinds

attack. This is a different matter (the sentence here is for a lack of loyalty to shareholders). And some have also pointed out that the fines (about 1 million dollars) are low for such large companies.

Another example is CISA's Secure By Design initiative, which encourages vendors to implement a series of good security practices. Rather than assigning legal responsibility, this softer approach asks vendors to voluntarily adhere to a set of virtuous pledges. Nearly 300 companies have already signed up.

2.6.2 *Efforts by some vendors*

Security equipment vendors are of course well aware that the many attacks observed since 2019 on edge equipment (and VPN servers in particular) is a serious problem. What's more, they're under huge pressure to provide urgent solutions following an attack involving their products.

As mentioned above, many of them have made (moral) commitments to provide more secure solutions. While not downplaying the importance of such commitments, we also note other, more concrete improvement actions:

- **Sophos** explained in its **Pacific Rim study** (which we mentioned in § 2.3.2 above, see also the article in our monthly bulletin) that it could protect its customers more effectively if it had more control over their Sophos firewall devices (in terms of data collection, supervision and even deployment of urgent patches). This proposal makes sense, because Sophos is well placed to observe and counter "global" attacks targeting Sophos equipment (e.g. with a wave of zero-day attacks). But it also raises a number of issues (for example, loss of sovereignty for the client company and the risk of failure if an automatic update is pushed at an inappropriate timing). However, it can be compared to cloud service models, where responsibility for maintaining the platform is entrusted to the provider: if a clearly outlined agreement (contractual, technical, etc.) is in place, and if clients trust their firewall provider, it could commit to managing the firewalls installed at client premises (ensuring security maintenance).

- **Palo Alto Networks** stated, in relation to attacks exploiting the zero-day vulnerability CVE-2024-0012 (in November 2024, see our alert CERT-IST/AL-2024.019), that it regularly scans the internet to identify Palo Alto Networks devices where the administration interface is exposed on the internet (a security risk) and that it notifies affected customers. This proactive approach to customer protection seems to us a new and welcome development.

3 Cert-IST activity in 2024

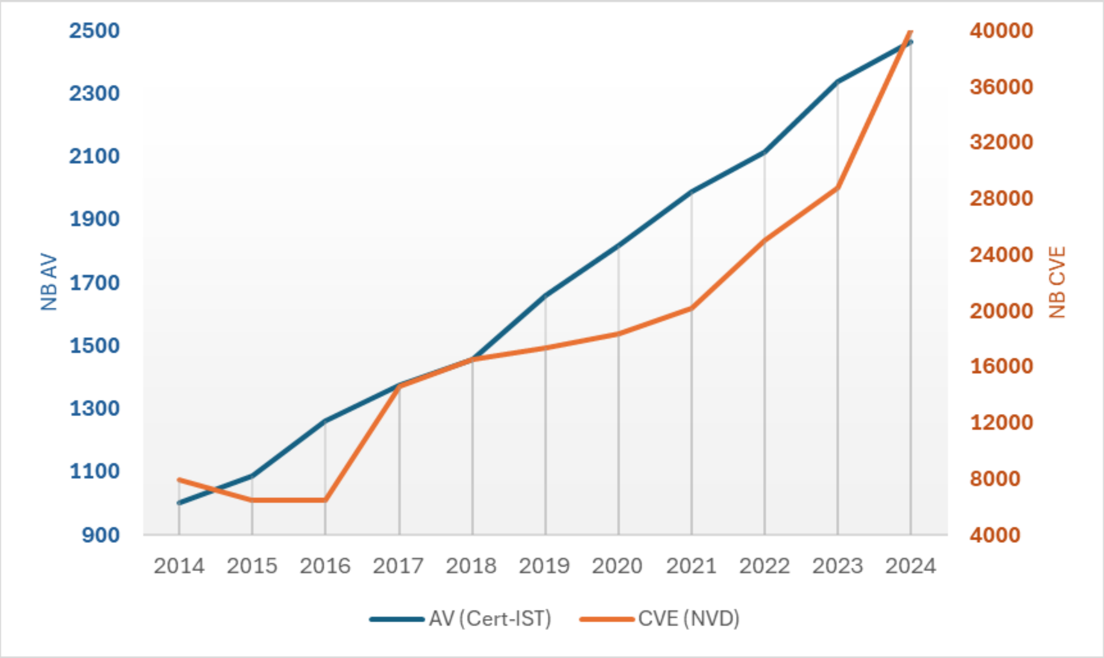
3.1 Vulnerability and threat feeds

As part of its monitoring of vulnerabilities and threats, Cert-IST produces various types of publications:

- **Security Advisories (AVs)**, which describe any newly discovered vulnerabilities in the products we monitor. Each AV deals with a set of CVEs.
- **Alerts (ALs)** are issued when there's a high risk of an attack on a vulnerability. **Info messages** are issued for notable but less dangerous events (e.g. media hype about a vulnerability).
- **Attack Reports (ATKs) and indicators of compromise (IOCs).** ATKs describe major attacks and hacker groups. The corresponding IOCs are made available in a MISP database. Both covers all kind of threats, including recurrent threats (malspam, botnets, ransomware), cyberespionage incidents (APT attacks) and the most significant ransomware.

The rest of this section provides a brief overview of publications in 2024.

3.1.1 Number of security advisories (and CVEs) published per year



Number of security advisories (and CVEs) published per year

3.1.2 Cert-IST alerts for 2024

Alert	Reference	Description	Date
Amber	CERT-IST/AL-2024.021	Attacks expected for Beyond Trust Remote Support (CVE-2024-12356)	11 Jan. 24
Yellow	CERT-IST/AL-2024.001	On-going attacks against Ivanti Connect Secure (ICS) (CVE-2023-46805, CVE-2024-21887, etc.)	12 Jan. 24
Yellow	CERT-IST/AL-2024.002	Ongoing attacks against GitLab (CVE-2023-7028)	23 Jan. 24
Yellow	CERT-IST/AL-2024.003	Ongoing attacks against Atlassian Confluence (CVE-2023-22527)	8 Feb. 24
Amber	CERT-IST/AL-2024.004	Attacks expected against devices running on FortiOS (CVE-2024-21762)	12 Apr. 24
Amber	CERT-IST/AL-2024.005	Ongoing attacks against devices running on PAN-OS (CVE-2024-3400)	26 Apr. 24
Amber	CERT-IST/AL-2024.006	Ongoing attacks against CrushFTP (CVE-2024-4040)	30 May 24
Yellow	CERT-IST/AL-2024.007	Ongoing attacks against Check Point VPN (CVE-2024-24919)	11 Jun. 24
Yellow	CERT-IST/AL-2024.008	Ongoing attacks against PHP on Windows (CVE-2024-4577)	2 Jul. 24
Yellow	CERT-IST/AL-2024.009	Attacks expected against OpenSSH (CVE-2024-6387)	18 Jul. 24
Yellow	CERT-IST/AL-2024.010	Expected attacks targeting Cisco Secure Email Gateway devices (CVE-2024-20401)	30 Aug. 24
Yellow	CERT-IST/AL-2024.011	Expected attacks against SPIP (CVE-2024-7954)	11 Sep. 24
Yellow	CERT-IST/AL-2024.012	Attacks expected for Microsoft Windows (CVE-2024-43491)	16 Sep. 24
Yellow	CERT-IST/AL-2024.013	Attacks expected for Ivanti Endpoint Manager (EPM) (CVE-2024-29847)	19 Sep. 24
Yellow	CERT-IST/AL-2024.014	Attacks expected on products using the Ruby-SAML library including GitLab (CVE-2024-45409)	27 Sep. 24
Yellow	CERT-IST/AL-2024.015	Attacks expected for Linux/Unix systems using CUPS (CVE-2024-47176, CVE-2024-47177, etc.)	2 Oct. 24
Amber	CERT-IST/AL-2024.016	Ongoing attacks against Zimbra Collaboration Suite (CVE-2024-45519)	24 Oct.24
Yellow	CERT-IST/AL-2024.017	Ongoing attacks against Fortinet FortiManager (CVE-2024-47575)	14 Nov. 24
Amber	CERT-IST/AL-2024.018	Attacks expected for Citrix Virtual Apps and Desktops (formerly XenApp and XenDesktop) with CVE-2024-8068 and CVE-2024-8069	18 Nov. 24
Yellow	CERT-IST/AL-2024.019	Ongoing attacks against Palo Alto Networks firewalls (CVE-2024-0012)	17 Dec. 24
Yellow	CERT-IST/AL-2024.020	Attacks expected against Apache Struts 2 (CVE-2024-53677)	20 Dec. 24

3.1.3 Attack Reports for 2024 (excluding recurring threats)

ATK	Name	Description
CERT-IST/ATK-2024.008	**UNC4841**	Cyberespionage group with potential links to the Chinese state.
CERT-IST/ATK-2024.012	**BianLian**	Cybercriminal group specialising in data theft and extortion.
CERT-IST/ATK-2024.013	**VexTrio**	Major cybercriminal affiliate programme based on traffic distribution systems (TDS).
CERT-IST/ATK-2024.014	**Blackwood**	Cyberespionage group targeting individuals and companies in China and Japan.
CERT-IST/ATK-2024.035	**Magnet Goblin**	Cybercriminal actor with expertise in exploiting one-day vulnerabilities.
CERT-IST/ATK-2024.039	**Earth Krahang**	Group of Chinese origin possibly linked to I-Soon and specialising in gaining initial access.
CERT-IST/ATK-2024.047	**CoralRaider**	Actor of Vietnamese origin motivated by financial gain.
CERT-IST/ATK-2024.056	**Black Basta**	Ransomware group targeting critical infrastructure in Europe and the United States.
CERT-IST/ATK-2024.057	**Ebury**	Persistent threat to Linux servers, targeting cryptocurrencies and financial data.
CERT-IST/ATK-2024.058	**Void Manticore**	Iranian actor combining destructive and influential operations.
CERT-IST/ATK-2024.060	**Doppelganger**	Pro-Russian disinformation campaign targeting Germany, France and other European countries.
CERT-IST/ATK-2024.070	**SneakyChef**	Cyberespionage group exploiting the Gh0st and SpiceRAT RATs.
CERT-IST/ATK-2024.082	**NullBulge**	Cybercriminal group claiming to defend artists against AI.
CERT-IST/ATK-2024.083	**Stargazer Goblin**	Actor organising malware distribution via GitHub.
CERT-IST/ATK-2024.092	**Silver Fox**	Cybercriminal group targeting critical sectors in China.
CERT-IST/ATK-2024.103	**Earth Baxia**	Sophisticated Chinese attacks on governments and companies in the APAC region.
CERT-IST/ATK-2024.104	**SloppyLemming**	Cybercriminal group using the cloud for espionage in South and East Asia.
CERT-IST/ATK-2024.114	**UAC-0184**	Spear phishing campaigns targeting Ukrainian defence forces.
CERT-IST/ATK-2024.125	**Emennet Pasargad**	Iranian company close to the IRGC conducting disinformation and destabilisation operations, including hack-and-leak.
CERT-IST/ATK-2024.126	**Mysterious Elephant**	APT-type group targeting governments and the public in South Asia.
CERT-IST/ATK-2024.137	**Head Mare**	Hacktivist group targeting Russia and Belarus with ransomware.

3.2 Technology monitoring

In addition to vulnerability tracking, Cert-IST also produces technology monitoring reports:

- **Daily media watch bulletin (press review)** listing the most relevant articles about security issues posted on French and English language websites.
- **Monthly SCADA watch bulletin** providing a summary of current events related to the security of industrial systems.
- **Monthly general bulletin** summarising the month's developments (in terms of vulnerabilities and attacks) and addressing current events with articles written by the Cert-IST team.
- **Monthly bulletin on attacks and IOCs**, which summarises the most significant events in the attack landscape.

4 Conclusions

A continuation of the trends seen in 2023

Overall, 2024 confirms the trends of previous years, but with a few notable developments.

Attacks on edge devices (such as Ivanti ICS and Fortinet) was the most significant development of the year. In 2023, we highlighted the difficulty of disinfecting targeted equipment and asked the question: Repair or simply replace? In 2024, these deep attacks continued and became even more widespread. No manufacturer seems to have been spared, with attacks against Check Point, Cisco, Fortinet, Ivanti, Juniper, Palo Alto Networks, SonicWall and Sophos. In response to this trend, we observed growing demand in 2024 from users and government bodies for **vendors to improve the quality of their products and take steps to curb these repeated compromises**. This has translated in Europe into a call for vendors to be made legally liable, and in the United States for them to commit to best practices (cf. CISA's Secure By Design initiative). We discussed both approaches in § 2.6.

On the cybercrime front, attacks continued unabated. Ransomware (including data enryption and data disclosure blackmail) remained the most common and publicised threat. After a peak of activity in 2023, the LockBit group largely declined in 2024 (it claimed responsibility for just four attacks in the last quarter). This is one of the effects of the **record number of arrests and takedown operations** by law enforcement agencies in 2024. The void left by LockBit was unfortunately quickly filled by other attacker groups (in particular **RansomHub**). But the legal action conducted in 2024 is putting a definite strain on this ecosystem and reversing the trend of virtual impunity they had enjoyed in recent years.

In addition to attacks by **infostealers** (still prevalent since 2022), we observed an increase in **phishing attacks targeting Microsoft 365** using **PhaaS** (phishing-as-a-service) kits such as **Tycoon 2FA**. These tools are capable of bypassing standard MFA protection mechanisms by implementing the **AitM** (adversary-in-the-middle) attack vector. To prevent them, stronger protection is needed, with phishing-resistant MFA solutions.

On the state-sponsored front, attacks by the **Big 4 (China, Russia, North Korea, Iran)** were the most publicised. As in 2023, China was omnipresent in the news. And in 2024, it was particularly the **offensive cyber ecosystem established by the Chinese government** which was described (zero-day collection, cyber-offensive companies like I-Soon, the ORB botnet, etc., see § 2.3.2).

Another feature of 2024 was the **large number of influence operations** (**Info Ops**, also call **FIMI** in Europe) carried out by certain states, most notably Russia and Belarus, but also Iran, China and Azerbaijan.

Areas of concern for 2025

In our opinion, the two issues likely to cause most concern for companies in 2025 will be:

- **Attacks on security appliances**, such as firewalls and VPNs, and against less-monitored devices more generally, which are internet-exposed but typically don't have EDR. One of the primary attention here is to ensure that these devices aren't overlooked in terms of monitoring. For example, detecting operational anomalies, monitoring platform integrity and monitoring traffic originating from these devices (rather than transit traffic), are areas that need to be strengthened.

- **Cloud security.** This vast and complex field is an increasingly central component of corporate information systems today. Attacks here are growing. And many areas need to be covered. They include:

    - Identity and access management.

    - The technical complexity of solutions deployed by companies.

    - The security level of SaaS solutions used.

Other important issues we note for 2025 include:

- Supply chain security.

- New regulatory frameworks (NIS2 and CRA).

- Identification of threats arising from the rollout of AI-powered solutions.

Strengthening intrusion detection and response

2024 showed once again that some attackers can be highly capable (cf. some of the state-sponsored attacks described in § 2.3) and that some security equipment can have easily exploitable zero-day vulnerabilities (hence the new buzzword "unforgivable vulnerability"). **Consequently, companies need to be prepared for successful intrusions.**

This means increasing security at every stage of the intrusion process:

- Upstream, by pursuing security efforts, in particular the due application of security patches.

- On detection of successful intrusions, for example using cyber decoys (canary tokens, honey tokens, etc.).

- Downstream, by training in cyber crisis management.

Cert-IST

290 Allée du lac
31670 Labège
France

info@cert-ist.com

https://www.cert-ist.com

+33 5 34 39 44 88