



CERT-IST

INDUSTRIE | SERVICES | TERTIAIRE

Cert-IST 2026 report on attacks and vulnerabilities in 2025

Released: March 2026

Contents

1	Introduction.....	3
2	Analysis of the most significant phenomena in 2025	4
2.1	Three key events of the year	4
2.1.1	ToolShell crisis: SharePoint on red alert.....	4
2.1.2	Targeting the “guardians”: F5 and Red Hat Consulting.....	4
2.1.3	Compromise of delegated identity: the Salesforce wave.....	5
2.2	The actors behind the attacks.....	6
2.2.1	State-sponsored groups: espionage, prepositioning and hybrid operations	6
2.2.2	Cybercrime: extortion, industrial disruption and data theft	7
2.2.3	Hacktivism: massive volume, informational impact.....	8
2.2.4	Blurred boundaries between these groups.....	8
2.3	Software supply chain integrity put to the test	9
2.4	Human infiltration and the insider threat.....	9
2.5	Zero-days and exploitation of edge devices	10
2.6	DDoS: crossing a new power threshold	11
2.7	Social engineering: automation and new techniques.....	11
2.8	Artificial intelligence: an operational accelerator.....	12
2.9	Cryptoasset theft still at prominent levels.....	12
3	Cert-IST activity in 2025.....	14
3.1	Vulnerability and threat feeds	14
3.1.1	Number of security advisories (and CVEs) published per year	14
3.1.2	Cert-IST alerts for 2025.....	15
3.2	Attack and IOCs watch	16
3.2.1	Campaigns and IOCs at a glance	16
3.2.2	Attack reports published in 2025	17
3.3	Technology monitoring	17
4	Conclusions.....	18

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.

2025 represented not so much a technological turning point as the culmination of a shift toward industrial-scale attack capabilities. The traditional “perimeter” model continued to erode, with attackers establishing a lasting foothold inside networks by compromising the “guardians” of the infrastructure, or even physically infiltrating IT teams through fraudulent recruitment methods. Our report also documents the maturity of AI agents, which have moved beyond the role of assistants to become autonomous operators.

Our report begins with an analysis of the key security phenomena throughout the year (see § 2). We then 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 2026.

➤ About Cert-IST

Cert-IST (Computer Emergency Response Team – Industry, Services, 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 safe return to normal operations.

Cert-IST 2026 report on attacks and vulnerabilities in 2025		Page: 3 / 19
TLP:CLEAR	CERT-IST-P-ET-26-001-EN	1.0

2 Analysis of the most significant phenomena in 2025

2.1 Three key events of the year

2025 marked a notable shift in the nature of the targets attacked. After the edge devices we highlighted in our 2024 vulnerability review (which nonetheless remained highly relevant in 2025), the most strategic attacks now appear to have focused on on-premises critical infrastructure, the trusted “custodians” of client secrets, and delegated SaaS identities.

Three major incidents illustrate this development.

2.1.1 ToolShell crisis: SharePoint on red alert

The most significant event involving a “traditional” vulnerability was the exploitation, during the summer of 2025, of the [ToolShell](#) chain affecting **on-premises Microsoft SharePoint Server**. This unauthenticated remote code execution flaw prompted Cert-IST to issue a [Red Alert](#) on 24 July an exceptional measure not seen since the [ProxyLogon](#) / [ProxyShell](#) crisis affecting Microsoft Exchange servers in 2021.

The timeline of this crisis clearly shows how rapidly a vulnerability can now be weaponised. First demonstrated at the Pwn2Own conference in May, it was patched by Microsoft on 8 July and reproduced by [Code White on 14 July](#). Only three days later, on 17 July, attacks were already leveraging a bypass of the original patch. Microsoft was forced to respond urgently on 19 July with a second, hardened fix. The full cycle was therefore completed in less than 10 days.

However, ToolShell’s most formidable aspect was likely the theft of SharePoint cryptographic keys, enabling attackers to forge legitimate authentication tokens. Once exfiltrated, these keys gave attackers persistent access even after patching. The only reliable remediation was a complete manual rotation of keys across the entire SharePoint farm an especially complex operation in a production environment.

2.1.2 Targeting the “guardians”: F5 and Red Hat Consulting

2025 confirmed a notable shift in initial intrusions: direct attacks against service providers that hold the blueprints of client infrastructure or have privileged access to client systems. These attacks illustrate a shift in supply chain risk. Beyond the SolarWinds style of software compromise, service providers themselves consultants and equipment vendors alike are increasingly becoming strategic targets.

In August, tech company **F5 Inc.** discovered a [long-running intrusion](#) conducted by the Chinese threat group [UNC5221](#) ([CERT-IST/INFO-2025.026](#)). After remaining in the company’s systems for more than a year, the attackers exfiltrated BIG-IP source code and information on internal vulnerabilities that had not yet been patched. The incident compelled F5 to release [44 emergency fixes](#) in October compared with only six in the previous quarter to mitigate the risk of future zero-day attacks.

Almost simultaneously, in early October, **Red Hat’s consulting business** suffered an [exfiltration](#) of 570 GB of data from its internal GitLab instance ([CERT-IST/INFO-2025.024](#)). The [Crimson Collective](#) group stole more than 28,000 repositories, including around 800 Customer Engagement Reports (CERs). These CERs contained network diagrams, authentication tokens, API keys and infrastructure configurations for critical clients, including HSBC, Walmart, Bank of America, Verizon, JP Morgan and the US Navy.

By targeting the service or equipment provider, attackers can easily gain complete visibility into the defences of hundreds of organisations at once. A single point of compromise can therefore turn into a large-scale supply chain risk, with every client of the “guardian” potentially within reach without any direct attack.

Cert-IST 2026 report on attacks and vulnerabilities in 2025		Page: 4 / 19
TLP:CLEAR	CERT-IST-P-ET-26-001-EN	1.0

2.1.3 *Compromise of delegated identity: the Salesforce wave*

The 2025 Salesforce crisis affected hundreds of organisations, even though no vulnerability in the CRM platform itself was exploited. By targeting third-party applications integrated with Salesforce, attackers triggered a series of cascading compromises.

The attackers believed to be the extortion group **ShinyHunters** (tracked by Google as [UNC6395](#)) first compromised [Salesloft's GitHub environment](#) between March and June before gaining access to its AWS infrastructure. Among other assets, this infrastructure hosted OAuth tokens linked to Drift, a marketing automation and conversational chat platform integrated with Salesforce. Using these tokens to authenticate to client environments, the attackers exfiltrated data from more than 700 organisations between 8 and 18 August, including Google, Cisco, Cloudflare and Gainsight.

The compromise of Gainsight proved particularly strategic. In November, the attackers used credentials stolen during the August attack to breach Gainsight's own infrastructure, giving them access to the OAuth tokens the company used for its Salesforce integrations. This led to the compromise of around [285 additional instances](#), affecting companies including Verizon, GitLab, F5 and SonicWall.

In parallel with these supply chain attacks, **ShinyHunters** also carried out a [vishing](#) campaign directly targeting employees at companies using Salesforce. By impersonating technical support, the attackers convinced victims to authorise fraudulent OAuth applications, thereby securing direct access to their Salesforce instances. In October, the group launched an [extortion site](#) naming 39 victims including FedEx, Disney, Toyota, Marriott, Air France-KLM, LVMH, Chanel, and issued a deadline of 10 October, threatening to release around 1 billion stolen records.

These intrusions illustrate the dangers posed by OAuth tokens. Once compromised, they bypass multifactor authentication, generate seemingly legitimate API traffic and enable attackers to operate for weeks without triggering any alerts.

Cert-IST 2026 report on attacks and vulnerabilities in 2025		Page: 5 / 19
TLP:CLEAR	CERT-IST-P-ET-26-001-EN	1.0

2.2 The actors behind the attacks

2025 confirmed the growing convergence of state-sponsored espionage, cybercrime and hacktivism. This hybridisation is clearly reflected in the targets, tools and tradecraft involved.

2.2.1 State-sponsored groups: espionage, prepositioning and hybrid operations

State-sponsored attacks take many forms, but they differ from other operations by their highly sophisticated capabilities and their stealth, with the aim of maintaining a long-term presence within the targeted organisation (prepositioning attacks).

The Big Four most cited states in our reports remain unchanged: China, Russia, North Korea and Iran. We note, as in 2024, that little is said about attacks by all the other states, especially the offensive cyber operations by Western countries.

China, [described by US intelligence](#) as «the most active and persistent cyberthreat», carried out several large-scale campaigns. In [July](#), three Chinese groups exploited the zero-day vulnerabilities involved in the ToolShell campaign (discussed in § 2.1.1) to compromise [more than 400 organisations](#) worldwide. The **Storm-2603** group stood out by deploying Warlock ransomware on US government servers, affecting in particular the National Nuclear Security Administration, the National Institutes of Health and the Department of Homeland Security. At the same time, **Salt Typhoon** continued its [telecommunications espionage campaign](#) by compromising at least 200 companies in 80 countries. In [December](#), the group breached the messaging systems used by staff of several committees of the US House of Representatives. Another major Chinese group, **Volt Typhoon**, also [continued its prepositioning operations](#) in critical infrastructure in 2025, focusing in particular on energy, transportation and telecommunications systems with a view to potential sabotage in the event of a geopolitical crisis.

Russia continued its hybrid campaigns. The **APT28** group conducted a [sustained campaign](#) against Western logistics and technology entities. In late December, **Sandworm** [attempted an attack](#) on the Polish power grid, deploying the destructive malware DynoWiper. At the same time, Russia stepped up its influence operations through [Doppelgänger](#), a disinformation campaign targeting, in particular, the German elections.

Iran was particularly active in 2025, with a [133% increase in cyberattacks](#) in May and June in connection with the conflict with Israel and the US-Israeli strikes (12-day war). The **MuddyWater** group conducted an [espionage campaign](#) targeting more than 100 government entities across the Middle East and North Africa. The group demonstrated a [significant evolution](#) in its offensive capabilities, including the deployment of the new MuddyViper backdoor.

Lastly, **North Korea** continued to blur the lines between cyberespionage and cybercrime. The attack on the [Bybit exchange platform in February](#), attributed to the **Lazarus** group, resulted in the theft of approximately \$1.5 billion in cryptocurrency. It reflects a model of state financing through cybercrime, conducted with a level of sophistication comparable with traditional espionage operations.

Cert-IST 2026 report on attacks and vulnerabilities in 2025		Page: 6 / 19
TLP:CLEAR	CERT-IST-P-ET-26-001-EN	1.0

2.2.2 Cybercrime: extortion, industrial disruption and data theft

Ransomware and extortion attempts more broadly [remained the most damaging threat](#) to businesses in 2025, although the landscape underwent a clear reshaping. Major coordinated law enforcement operations led by Europol since 2024 ([Operation Cronos against LockBit](#) and [Operation Endgame against distribution botnets, loaders and infostealers](#)) have fragmented this ecosystem. **RansomHub**, which had filled the vacuum left by **LockBit**, [disappeared in late March 2025](#), likely as a result of internal disputes. [LockBit resurfaced in September 2025](#) with LockBit 5.0, announcing the [formation of a cartel with Qilin and DragonForce](#) to share techniques, resources and infrastructure.

Cybercrime is also being reshaped by increased corporate awareness: the average ransom payment rate [fell to 23% in Q3 2025](#), a historic low.

Large-scale RaaS operations gave way to a myriad of smaller groups (between 126 and 141 were active in 2025, compared with 70 in 2023), while closed groups such as **Akira** and **Play** continue to survive through a volume-based strategy involving lower ransom demands and targeting less mature mid-sized companies. Geographic expansion is also accelerating: ransomware now accounts for [51% of incidents in the Asia-Pacific region](#), which had previously been less exposed than North America or Europe.

From a tactical standpoint, 2025 saw the continued rise of extortion without encryption. The campaign carried out by **CIOp** against Oracle E-Business Suite is a clear example: [zero-day exploitation](#) of vulnerabilities, data theft reaching up to 180 GB per victim and more than 100 organisations affected, including Harvard, Dartmouth, Logitech and Korean Air. Oracle's chaotic communication management (a silent patch in July, followed by emergency alerts in October) gave attackers a three-month window of exploitation during which many organisations remained unaware of their exposure.

The Jaguar Land Rover case also illustrates the scale of the financial losses that can arise from an attack on a sensitive environment. Conducted by [Scattered Spider / Lapsus\\$ Hunters](#), it caused a five-week production shutdown at a total cost of more than [\\$2.5 billion](#), showing how an IT intrusion can readily paralyse OT environments without any direct sabotage. Other sectors were affected by similar attacks, whose operational impact combined with government sanctions can run into several hundred million euros, as shown by [Bouygues Telecom](#), [Marks & Spencer](#) and [SK Telecom](#).

In the healthcare sector, the February 2024 [Change Healthcare](#) incident was confirmed in 2025 as the largest data breach ever recorded, exposing the data of 192.7 million Americans. Its impact went far beyond the data leak itself, disrupting medical payments across the United States for several months and exposing the risks of a dangerous systemic dependence on a highly centralised system.

From a technical perspective, cybercriminals appear to have moved away from zero-day attacks in favour of phishing and the use of stolen credentials (see also § 2.7). Information-stealing malware is feeding an ecosystem of initial access brokers, who resell compromised credentials to ransomware groups.

Lastly, phishing-as-a-service, with turnkey kits such as Tycoon 2FA, FlowerStorm and Darcula, continues to make it easier to bypass multifactor authentication through adversary-in-the-middle techniques.

Cert-IST 2026 report on attacks and vulnerabilities in 2025		Page: 7 / 19
TLP:CLEAR	CERT-IST-P-ET-26-001-EN	1.0

2.2.3 Hactivism: massive volume, informational impact

According to the European Union Agency for Cybersecurity (ENISA), hactivism accounted for [80% of cyber incidents in Europe](#) in 2025. Pro-Russian groups dominated the landscape, with **NoName057(16)** responsible for more than 60% of DDoS claims through its DDoSia platform. [Operation Eastwood](#), coordinated by Europol in July 2025, temporarily disrupted the group's infrastructure, but unfortunately did not prevent its rapid recovery.

In France, the [NoName057\(16\) collective claimed responsibility](#) for the attack on La Poste on 22 December, disrupting banking and postal services during the festive period. The technical impact generally remained limited, but these operations are part of a strategy of sustained informational pressure, amplified by social media and public claim channels.

Hactivism is also evolving beyond simple DDoS attacks. Groups such as [Z-Pentest](#), for example, are targeting industrial systems. Researchers reported a [twofold increase](#) in such attacks in Q3 2025, with nearly a quarter targeting OT (operational technology) environments, especially in the water, agriculture and energy sectors.

In the Middle East, the pro-Israeli group **Predatory Sparrow** struck [Nobitex, Iran's largest cryptocurrency platform](#) in June, draining \$90 million. The funds were transferred to inaccessible addresses, making recovery impossible (a deliberate act of destruction for political purposes). Nobitex, which accounts for 87% of Iran's crypto trading volume, was accused of facilitating sanctions evasion and financing groups affiliated with the Islamic Revolutionary Guard Corps (IRGC).

2.2.4 Blurred boundaries between these groups

The traditional distinction between state actors, cybercriminals and hactivists is becoming more blurred than ever. Russia [directly finances and directs](#) cybercriminal and hactivist groups: the GRU controls **NoName057(16)** and **CARR** through dedicated officers, while the FSB [recruits convicted hackers](#) and turns them into operational assets.

In 2025, [North Korea stole \\$2.02 billion](#) in cryptocurrency, in particular to fund its nuclear programme, further blurring any distinction between espionage and cybercrime.

Iran presents a hybrid model: the [Pioneer Kitten group conducts espionage operations and sells the resulting access](#) to Russian ransomware groups in order to monetise its intrusions.

Lastly, a fourth category is gaining strength: **"hackers for hire"** cyber mercenaries who work indiscriminately for states, cybercriminals or companies. No fewer than [74 governments](#) have used cyber mercenaries for the deployment of spyware alone, in a market already valued at \$12 billion as early as 2019. These actors, whose sophistication is comparable to state intelligence services, are creating growing confusion in the attribution of attacks.

Cert-IST 2026 report on attacks and vulnerabilities in 2025		Page: 8 / 19
TLP: CLEAR	CERT-IST-P-ET-26-001-EN	1.0

2.3 Software supply chain integrity put to the test

Software development is playing an increasingly significant role in intrusion strategies. 2025 revealed a methodical diversification of attack vectors, whose effectiveness relies on a multiplier effect: compromising a maintainer or a tool makes it possible to reach thousands of organisations simultaneously.

Highly targeted phishing campaigns against packages and modules maintainers were observed. In September, for example, [Josh Junon \(Qix-\)](#), maintainer of **NPM** libraries accounting for 2.6 billion weekly downloads, including **chalk** and **debug**, fell victim to a campaign that bypassed his two-factor authentication. During the two-hour compromise window, 2.5 million downloads distributed malicious code, with each installation potentially corresponding to an infected production application.

Conversely, self-propagating techniques are amplifying these compromises. The [Shai-Hulud](#) worm reused the credentials stolen during the [S1ngularity incident](#) in August to automatically inject itself into hundreds of packages. It then steals API keys, AWS secrets and GitHub tokens from new developers, creating an exponential infection cycle.

Lastly, developers' workstations have themselves become entry points, following intrusions of growing sophistication. In October, for example, the [GlassWorm campaign](#) turned Visual Studio Code extensions (Microsoft's code editor) into trojanized components that deployed remote access and proxy functions.

However, the multiplier effect referred to above reaches its peak when attackers directly target shared cloud infrastructures. In March, [CloudSEK disclosed](#) what it described as the largest supply chain attack of 2025: 6 million records stolen from [Oracle Cloud](#) authentication servers. The compromised data reportedly included encrypted passwords, certificates and access keys belonging to 140,000 tenants, creating a domino effect that could enable access to the cloud environments of thousands of companies. [Oracle firmly disputed the claims](#) despite the evidence published, creating an unprecedented degree of uncertainty as to the true scale of the incident.

To mitigate the impact of similar attacks in the future, a range of technical responses has been introduced, mainly by code hosting platforms. In September, GitHub rolled out temporary token authentication for NPM, a measure that could have significantly curtailed the S1ngularity and Shai-Hulud campaigns had it been deployed earlier. **PyPI**, the Python software repository, is accelerating the deployment of automatic quarantine mechanisms for suspicious packages.

However, protections at the public repository level are not always enough, and in our view, companies must now take account of this risk. Measures to be considered include scanning and validating open-source dependencies through an independent system, potentially AI-enabled, as well as maintaining an internal code registry.

2.4 Human infiltration and the insider threat

Several major incidents in 2025 illustrated how organisational trust can be exploited as an intrusion vector.

First, in terms of **infiltration**, the ongoing North Korean [Wagemole](#) campaign deserves particular mention. This campaign has now been active for several years: North Korean operatives secure employment within Western companies under false identities, using generative AI to produce convincing CVs and profile pictures. During recruitment video interviews, real-time deepfake technology is used to replace faces.

Cert-IST 2026 report on attacks and vulnerabilities in 2025		Page: 9 / 19
TLP: CLEAR	CERT-IST-P-ET-26-001-EN	1.0

US authorities uncovered “laptop farms” in [at least 16 states](#): local accomplices receive the company-issued equipment and, once it has been configured, enable remote access from North Korea. The redirected salaries go on to fund the Pyongyang regime.

The [Contagious Interview](#) campaign, also attributed to North Korea, exploits the recruitment processes of Western companies to target external candidates. Developers are lured into fake interviews where they are prompted to install “technical tests” or run commands to “fix” a malfunctioning webcam. Between June and July 2025, more than 17,000 downloads of malicious NPM packages were attributed to this campaign.

From an **insider threat** perspective, the Coinbase incident a major financial company specialising in cryptocurrencies is symptomatic of increasingly worrying scenarios. A [support employee](#) was arrested for facilitating access to the data of 69,461 clients.

At [CrowdStrike](#), an employee sold screenshots of internal systems for \$25,000.

At the [Central Bank of Brazil](#), credentials sold for just \$920 enabled the theft of \$140 million.

And an [intrusion at Coupang](#) (South Korea’s equivalent of Amazon) was traced back to a former employee who had retained access after leaving the company.

These compromises show that, although detection techniques continue to improve, social engineering can be used to circumvent them, regardless of their sophistication. As a result, recruitment processes, continuous identity verification and the strict revocation of access rights are now security issues every bit as critical as security event detection and perimeter protections.

2.5 Zero-days and exploitation of edge devices

As in 2024, the exploitation of vulnerabilities affecting edge devices continued at a sustained pace in 2025. Of the **27** alerts issued by Cert-IST during the year, **16 concerned such devices** (59.3%), confirming that VPNs, firewalls and various appliances remain not only a hunting ground of choice for attackers, but also the leading cause of crisis activation at Cert-IST.

This concentration comes as no surprise: by design, these devices are exposed to the internet and are rarely equipped with EDR solutions, which makes forensic analysis more difficult and facilitates long-term compromise.

[ENISA](#) confirms that **vulnerability exploitation** accounts for 21.3% of intrusion vectors in Europe (it should be noted that the vast majority of intrusions are still attributed to phishing and social engineering). A [report by NSHC ThreatRecon](#) also observes that around half of the vulnerabilities exploited in 2025 were new and that nearly one third were weaponised on the very day their CVE was published or even earlier in the case of zero-days.

The usual targets remained unchanged: Ivanti Connect Secure ([AL-2025.001](#), [AL-2025.008](#)), Fortinet FortiOS and FortiWeb ([AL-2025.002](#), [AL-2025.016](#)), Cisco ASA/FTD ([AL-2025.019](#)), Palo Alto Networks ([AL-2025.003](#)), NetScaler ([AL-2025.014](#), [AL-2025.018](#)) and SonicWall ([AL-2025.010](#)).

This industrialisation of vulnerability exploitation, now within reach of threat actors at all levels, continues to demand a high degree of responsiveness from companies, along with constant visibility into their exposed assets.

Cert-IST 2026 report on attacks and vulnerabilities in 2025		Page: 10 / 19
TLP: CLEAR	CERT-IST-P-ET-26-001-EN	1.0

2.6 DDoS: crossing a new power threshold

Here too, 2025 marked a dramatic leap in scale. DDoS attacks, which had already reached a peak of **5.6 Tbps** at the end of 2024, set new records in 2025: **29.7 Tbps** in September, then **31.4 Tbps** in December a sixfold increase in the space of a year. The [Aisuru](#) botnet, with 1 to 4 million compromised connected devices, was the main driver behind these records.

This increase in power was matched by an explosion in the number of attacks: Cloudflare recorded **47.1** million attacks in 2025, compared with **21.3** million in 2024. Yet these striking figures should not obscure the operational reality: most attacks remain very short-lived (often lasting less than a minute) and are automatically mitigated by specialised protection providers.

We would therefore argue that the main issue lies in the accessibility of these attacks. Thanks to DDoS-for-Hire services, virtually anyone can rent multi-Tbps attack capacity for just a few hundred dollars. Law enforcement is, of course, responding, with operations such as [PowerOFF](#) (27 platforms dismantled in December 2024) and [Eastwood](#) (which disrupted the NoName057(16) group in July 2025). These tactical successes can temporarily slow operations, but they almost never manage to eradicate a botnet entirely.

For companies, the key issue is therefore not so much the maximum power of attacks as their level of preparedness: having appropriate, automated protection capable of absorbing multi-Tbps volumes remains the only effective safeguard against an industrialised, day-to-day threat.

2.7 Social engineering: automation and new techniques

Social engineering remains the leading **intrusion vector**, accounting for [60% of incidents](#) recorded by ENISA in 2025. Beyond traditional phishing, the year also saw the emergence of techniques that bypass conventional defences by directly exploiting trust or internal processes.

The [ClickFix](#) phenomenon, first observed in spring 2024, surged dramatically in 2025 (**+517%**). These attacks display fake error messages (Windows updates, CAPTCHAs, security warnings) and prompt the user to execute commands themselves in order to “resolve” the issue. As a result, victims install malware without attackers having to bypass any security controls. Initially targeting Windows, ClickFix expanded to macOS and Linux, deploying infostealers, RATs and backdoors. Variants such as [ConsentFix](#) even hijacked Azure OAuth authentication to obtain access tokens. By the end of the year, the paid-for platform ErrTraffic had commercialised the automation of these campaigns.

At the same time, [targeted vishing against helpdesks](#) became a method of choice for intrusion. The **Scattered Spider** group systematised this approach by impersonating legitimate employees when contacting support services, thereby obtaining account resets or access without having to compromise any systems. This technique enabled major intrusions at Marks & Spencer, Co-op and several US insurance companies. The **Cognizant** case, where Clorox sued the company for \$380 million after an attacker deceived its helpdesk, illustrates the financial consequences of such procedural failures.

Lastly, the release of a [mega-leak of 16 billion credentials](#) a massive aggregation of past breaches involving services such as Google, Apple and Facebook turned years of password reuse into a global reservoir for **credential stuffing** attacks. This database, which was readily accessible, mechanically amplified all identity-based attacks, making account compromise even more trivial.

Cert-IST 2026 report on attacks and vulnerabilities in 2025		Page: 11 / 19
TLP:CLEAR	CERT-IST-P-ET-26-001-EN	1.0

2.8 Artificial intelligence: an operational accelerator

AI is gradually shifting from the role of assistant to operational actor in cyber intrusions. In September, Anthropic disclosed the **GTG-1002** attacks, attributed to a Chinese state-sponsored group: by abusing Claude Code through roleplay techniques (convincing the model that it was carrying out legitimate security testing), the group automated 80% to 90% of the tactical operations targeting around 30 organisations.

The system orchestrated reconnaissance, vulnerability discovery, exploit generation, credential harvesting and data exfiltration, with human intervention limited to critical escalations. Its execution speed thousands of requests per second made any manual response impossible. This campaign constitutes the first documented case of a large-scale cyberattack driven primarily by AI.

On the enterprise side, the large-scale deployment of LLMs is opening up new attack surfaces. Prompt injection attacks manipulate model behaviour, with newly identified vulnerabilities such as:

- The potential for data leakage in [Microsoft 365 Copilot](#) through emails containing hidden prompts.
- A risk of data exfiltration through [Google Gemini](#) when manipulated via calendar invitations.
- Risks associated with compromised coding assistants, for example through [prompts concealed in project README files](#).

The [Amazon Q](#) case, meanwhile, was a genuine incident: a compromised VS Code extension, which remained online for nearly two days, contained a prompt instructing the deletion of local files and AWS resources accessible to the developer.

These developments require a rethink of defences: strict access controls for enterprise AI assistants and detection systems capable of addressing attack tempos that exceed human real-time analysis capabilities.

2.9 Cryptoasset theft still at prominent levels

2025 marked the third consecutive record year for cryptocurrency theft, with [more than \\$3.4 billion stolen](#), according to Chainalysis. Beyond the Bybit hack discussed above, losses were more broadly distributed: [Cetus](#) (\$223 million), [Phemex](#) (\$85 million) and [Nobitex](#) (\$80–90 million), while [158,000 individual wallets](#) were compromised for a total of \$713 million through phishing campaigns and other malware directly targeting users and their private keys.

North Korea remains the dominant state actor, with [\\$2.02 billion stolen](#) (59% of the total). However, its tactics have evolved. Shifting away from DeFi protocols, the regime is now increasingly targeting centralised exchanges through social engineering and by [infiltrating employees](#) under false identities, thereby securing legitimate access to key management infrastructure.

The laundering of stolen cryptocurrency is also highly structured, relying on networks of intermediaries based in Southeast Asia (brokers carrying out off-exchange transactions and parallel banking channels specialising in conversion into fiat currency). These actors fragment the funds through cross-chain transfers and mixing services, then cash them out gradually over several weeks, making it difficult to trace despite the native transparency of blockchains.

Cert-IST 2026 report on attacks and vulnerabilities in 2025		Page: 12 / 19
TLP: CLEAR	CERT-IST-P-ET-26-001-EN	1.0

Beyond state-sponsored operations, attacks on DeFi protocols continued unabated: exploitation of smart contract vulnerabilities, manipulation of price oracles and compromise of liquidity pools. Losses are becoming increasingly concentrated (the three largest hacks account for 69% of the total value stolen), even as the number of incidents continues to rise, revealing a fragmented threat landscape shaped by sophisticated state actors and opportunistic cybercriminals exploiting the sector's still immature security posture.

Cert-IST 2026 report on attacks and vulnerabilities in 2025		Page: 13 / 19
TLP:CLEAR	CERT-IST-P-ET-26-001-EN	1.0

3 Cert-IST activity in 2025

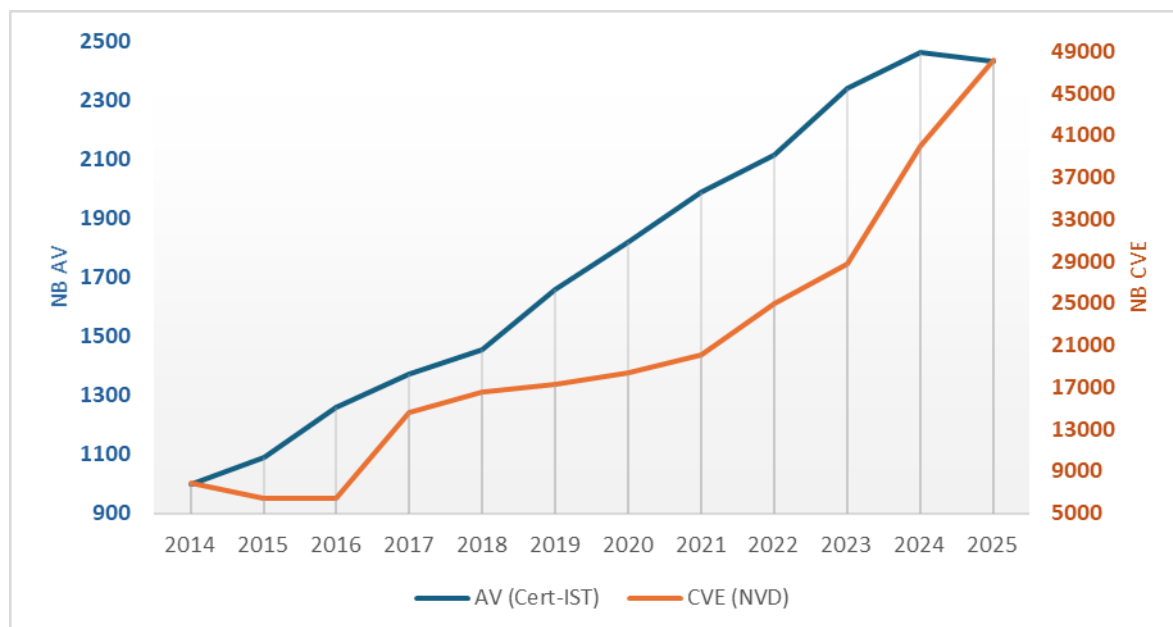
3.1 Vulnerability and threat feeds

As part of its monitoring of vulnerabilities and threats, Cert-IST produces several 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 is an elevated risk of an attack on a vulnerability. **INFO messages** are issued for notable but less dangerous events (e.g. high-profile vulnerabilities).
- **Attack Reports (ATKs) and indicators of compromise (IoCs)**. ATKs list major attacks and hacker groups. The corresponding IoCs are made available in a MISP database. IoCs refer to 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 2025.

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 2025

Alert	Reference	Description	Date
Amber	CERT-IST/AL-2025.001	Ongoing attacks on Ivanti Connect Secure (ICS) (CVE-2025-0282)	09 Jan 2025
Amber	CERT-IST/AL-2025.002	Ongoing attacks on Fortinet FortiOS (CVE-2024-55591)	15 Jan 2025
Yellow	CERT-IST/AL-2025.003	Ongoing attacks on Palo Alto Networks PAN-OS (CVE-2025-0108)	14 Feb 2025
Yellow	CERT-IST/AL-2025.004	Ongoing attacks on Apache Tomcat (CVE-2025-24813)	18 Mar 2025
Yellow	CERT-IST/AL-2025.005	Risk of attacks on GLPI	21 Mar 2025
Yellow	CERT-IST/AL-2025.006	Risk of attacks on the NGINX Ingress Controller for Kubernetes (CVE-2025-1974)	26 Mar 2025
Yellow	CERT-IST/AL-2025.007	Ongoing attacks on CrushFTP (CVE-2025-31161)	01 Apr 2025
Amber	CERT-IST/AL-2025.008	Ongoing attacks on Ivanti Connect Secure (ICS) (CVE-2025-22457)	04 Apr 2025
Yellow	CERT-IST/AL-2025.009	Ongoing attacks on Erlang OTP	25 Apr 2025
Yellow	CERT-IST/AL-2025.010	Ongoing attacks on SonicWall SMA100 (CVE-2024-38475 et CVE-2023-44221)	02 May 2025
Yellow	CERT-IST/AL-2025.011	Ongoing attacks on Commvault software (CVE-2025-34028)	05 May 2025
Amber	CERT-IST/AL-2025.012	Ongoing attacks on Ivanti EPMM (CVE-2025-4427, CVE-2025-4428)	15 May 2025
Yellow	CERT-IST/AL-2025.013	Risk of attacks on Fortinet FortiMail	27 May 2025
Amber	CERT-IST/AL-2025.014	Ongoing attacks on NetScaler ADC and NetScaler Gateway (CVE-2025-6543, CVE-2025-5777)	25 Jun 2025
Yellow	CERT-IST/AL-2025.015	Risk of attacks on Cisco Unified Communications Manager (CUCM equipment) (CVE-2025-20309)	03 Jul 2025
Yellow	CERT-IST/AL-2025.016	Ongoing attacks on Fortinet FortiWeb (CVE-2025-25257)	15 Jul 2025
Red	CERT-IST/AL-2025.017	Ongoing attacks on Microsoft SharePoint (#ToolShell)	21 Jul 2025
Yellow	CERT-IST/AL-2025.018	Ongoing attacks on NetScaler ADC and NetScaler Gateway (CVE-2025-7775)	27 Aug 2025
Amber	CERT-IST/AL-2025.019	Ongoing attacks on Cisco ASA and Cisco FTD (CVE-2025-20333, CVE-2025-20362)	26 Sep 2025
Amber	CERT-IST/AL-2025.020	Ongoing attacks on Oracle E-Business Suite (CVE-2025-61882)	06 Oct 2025
Yellow	CERT-IST/AL-2025.021	Ongoing attacks on the Windows Server Update Service (WSUS)	27 Oct 2025
Yellow	CERT-IST/AL-2025.022	Ongoing attacks on Fortinet FortiWeb (CVE-2025-64446, CVE-2025-58034)	14 Nov 2025
Yellow	CERT-IST/AL-2025.023	Ongoing attacks on Oracle Identity Manager (CVE-2025-61757)	24 Nov 25

Amber	CERT-IST/AL-2025.024	Ongoing attacks on internet-exposed React / Next.js applications (CVE-2025-55182) (React2Shell)	05 Dec 2025
Yellow	CERT-IST/AL-2025.025	Ongoing attacks on various Fortinet products (CVE-2025-59718, CVE-2025-59719, CVE-2026-24858)	17 Dec 2025
Yellow	CERT-IST/AL-2025.026	Ongoing attacks on Cisco Secure Email Gateway and Cisco Secure Email and Web Manager (CVE-2025-20393)	18 Dec 2025
Yellow	CERT-IST/AL-2025.027	Ongoing attacks on MongoDB	29 Dec 2025

3.2 Attack and IOCs watch

The Cert-IST attack and IoCs watch service tracks known attack campaigns, threat groups and their tactics, techniques and procedures (TTPs) and provides members with curated indicators of compromise (IoCs) through a MISP instance to feed into their detection and investigation systems.

3.2.1 Campaigns and IoCs at a glance

In 2025, Cert-IST processed **21,161 MISP events / campaigns**, a volume broadly stable compared with 2024. The number of **OSINT reports** analysed increased to **1,770** (up from 1,489 in 2024), while **144 attack reports (ATKs)** were produced, a level that has remained steady for several years.

The attack vectors identified across the campaigns analysed by **Cert-IST** remained largely dominated by social engineering: phishing (43.9%), frauds (21.3%) and malspam (19.4%) together account for more than **84%** of the vectors observed.

The most frequently observed malware families were **Remcos** (12.1%), **Formbook** (11.1%) and **AgentTesla** (10.4%). These three off-the-shelf tools are ubiquitous in the cybercriminal ecosystem.

Stealers and RATs accounted for 39% and 36% respectively of the malware types identified, confirming the continued priority given to information theft and remote takeover.

Among the **659 attributed events** (i.e. for which a threat group was identified), **Gamaredon** (Russia) ranked first (9.9%), ahead of the North Korean campaigns **Contagious Interview** (5.2%), **Lazarus** and **Kimsuky** (3.5% each).

Russia and North Korea account for the majority of state-linked attributions, although a notable presence of Chinese actors should also be highlighted (Mustang Panda, UNC5221).

3.2.2 Attack reports published in 2025

ATK	Name	Description
CERT-IST/ATK-2025.008	TA866	Hybrid actor operating at the intersection of cybercrime and cyberespionage since 2020.
CERT-IST/ATK-2025.021	Contagious Interview	North Korean cyberthreat targeting developers and IT recruiters.
CERT-IST/ATK-2025.031	RansomHub	Ransomware-as-a-Service (RaaS) operation that emerged in 2024, targeting companies through double extortion.
CERT-IST/ATK-2025.032	MirrorFace	Chinese cyber-espionage APT primarily targeting Japan through spear-phishing.
CERT-IST/ATK-2025.045	TraderTraitor	North Korean group targeting the crypto sector through recruitment lures and trojanized open-source code.
CERT-IST/ATK-2025.057	DOGE Big Balls	Group using the Fog ransomware, combining advanced techniques with political provocation.
CERT-IST/ATK-2025.069	CyberVolk	Pro-Russian hacktivist collective combining ransomware, data theft and DDoS attacks.
CERT-IST/ATK-2025.071	UAC-0226	Cyber-espionage operation targeting Ukraine using the GIFTEDCROOK malware.
CERT-IST/ATK-2025.102	ShinyHunters	Hacker group specialising in large-scale data breaches and extortion.
CERT-IST/ATK-2025.103	Liminal Panda	Chinese cyber-espionage group targeting mobile telecommunications operators since 2020.
CERT-IST/ATK-2025.117	UNC5221	Chinese group exploiting zero-day vulnerabilities in appliances for stealth intrusions.
CERT-IST/ATK-2025.119	UAC-0099	Spear-phishing activities targeting Ukraine through legal-themed messages.
CERT-IST/ATK-2025.132	PlushDaemon	Chinese APT group specialising in hijacking of software updates.
CERT-IST/ATK-2025.144	Earth Alux	Chinese APT group specialising in the exploitation of IIS and SharePoint servers.

3.3 Technology monitoring

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

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

Cert-IST 2026 report on attacks and vulnerabilities in 2025		Page: 17 / 19
TLP:CLEAR	CERT-IST-P-ET-26-001-EN	1.0

4 Conclusions

2025 served as a stark wake-up call, exposing the structural weaknesses of our digital ecosystem. More than a simple evolution of the threat landscape, it marked a shift toward the industrialisation of offensive capabilities, where system complexity has become the attacker’s most effective ally.

In our view, three key lessons emerge to help shape defence strategies in 2026.

1. **The collapse of the MFA “barrier” and the shift toward machine identity.** The first key lesson is the end of the relative immunity traditionally provided by multifactor authentication (MFA). The Salesforce incidents and the ToolShell attacks targeting SharePoint showed that attackers are no longer seeking so much to “break” a password as to “steal” already established trust. By targeting OAuth tokens and cryptographic secrets, groups such as ShinyHunters were able to bypass MFA systems and secure near-undetectable persistence. As a result, the priority for 2026 is no longer simply to protect human access, but to establish strict governance over non-human identities.
2. **The challenge of tempo: defence at machine speed.** The second key lesson concerns the acceleration of the attack cycle. With the emergence of operations such as [GTG-1002](#), in which AI agents handle most of the tactical workload, time has become an asymmetric factor. Faced with a machine capable of automating reconnaissance and exploitation, a manual human response is bound to fail. In 2026, reducing remediation time will therefore necessarily depend on the automation of defence: AI-based triage and orchestration are no longer optional, but operational imperatives.
3. **Extending Zero Trust to the supply chain and edge devices.** An organisation’s security is only as strong as the weakest link in its partner ecosystem. The compromise of Red Hat Consulting and the emergence of the [self-replicating Shai-Hulud worm](#) are reminders that **service providers** and **code repositories** have become aggregators of critical secrets. At the same time, edge devices often lacking EDR protection remain strategic blind spots.
In 2026, the Zero Trust approach must be extended without delay to third-party access and to integrity monitoring of exposed devices.

Lastly, the lessons of 2025 call into question the culture of “tool sprawl”. To address increasingly convergent threats, tomorrow’s resilience may well rest on three pillars:

1. **Simplicity:** Reducing the attack surface by streamlining SaaS interconnections and eliminating unnecessary privileges.
2. **Visibility:** Eliminating blind spots, whether they involve unsupervised edge appliances or access tokens delegated to third-party applications.
3. **Automation:** Enhancing detection and response to match the pace of offensive AI agents and protect critical assets in real time.

Cert-IST 2026 report on attacks and vulnerabilities in 2025		Page: 18 / 19
TLP: CLEAR	CERT-IST-P-ET-26-001-EN	1.0

CERT-IST

290 Allée du Lac

31670 Labège

France

info@cert-ist.com

<https://www.cert-ist.com>

+33 (0)5 34 39 44 88



Cert-IST 2026 report on attacks and vulnerabilities in 2025		Page: 19 / 19
TLP:CLEAR	CERT-IST-P-ET-26-001-EN	1.0