2025 Report

Trends and analysis of one year of incident response

By the CERT WAVESTONE

WAVESTONE

Who are we?

Wavestone: a high value-added consulting offering

360° Portfolio of best-in-class consulting services

17 countries A global strike force

+6 000 Employees

943,7 M€ Pro forma revenue

Independent Perspective & solution-based actions

CERT-Wavestone: 40 experts specialized in cyber crisis

During incidents...

- Investigations and forensic analysis
  System, network, and code analysis
- Crisis management
  Coordination, anticipation, support for internal and external communication, assistance with regulatory requirements
- Defense strategies
- Remediation and reconstruction
- Threat identification

...And upstream

- CSIRT staff augmentation
- CSIRT training
- Crisis exercises
- Cyberattack simulations
  RedTeam / Purple-team / Cyber Range
- SOC and CSIRT Evolution
  Maturity assessments, training, action plans
- Phishing campaigns
- Cyber resilience assessments
- Internet footprint evaluation
- Cyber Threat Intelligence

Wavestone was the first company to be awarded and renew the “Prestataire de Réponse aux Incidents de Sécurité" (PRIS-LPM) certification by ANSSI across all scopes:

- Search for Indicator of Compromise [REC]
- Digital Forensics [INV]
- Malicious code analysis [CODE]
- Forensics steering and coordination [PCI]

This report presents the analysis of 21 major incidents handled by CERT-Wavestone between August 2024 and September 2025, across a wide range of sectors including strategic enterprises, healthcare institutions, and higher education.

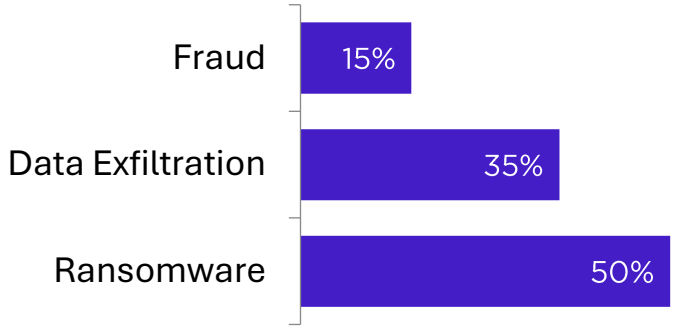
Financial gain: the primary motivation behind attacks

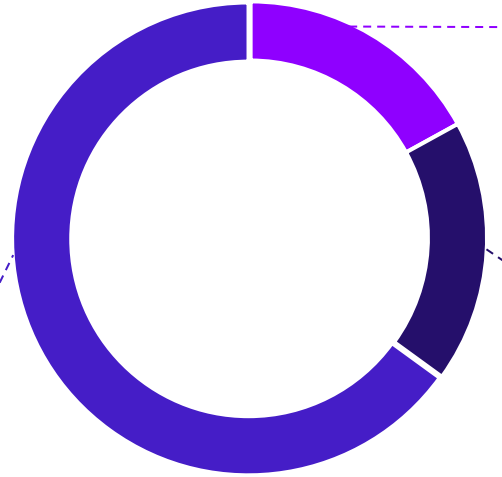
Ransomware and data exfiltration remain the top threats in 2025

Financial gain (65%)

Mainly through disabling information systems, extortion via the threat to disclose sensitive data, or fraud.

50% in 2024, 46% in 2023





Espionage (17%)

These attacks are increasingly frequent each year, driven by a tense geopolitical context.

10% in 2024, 8% in 2023

Unknown motivations(18%)

In some cases, the attackers' motives remain unclear, due to a lack of impact, early interruption of the attack or insufficient evidence.

35% in 2024, 29% in 2023

This year, CERT-Wavestone did not intervene in any insider threat cases, as these were mostly handled internally by our clients' teams.

These types of attacks accounted for 5% of interventions in 2024 and 6% in 2023.

Phishing and its variants: the primary entry point into information systems

38%

20% in 2024

Phishing, vishing, and use of stolen credentials

These methods often enable privilege escalation by impersonating IT support or compromising components such as ADCS, CI/CD pipelines, or hypervisor tools.

22%

20% in 2024

Intrusion via remote access systems (Citrix, VPN, etc.)

These provide direct access to the company's critical systems.

20%

40% in 2024

Exploitation of vulnerabilities in exposed web applications

These attacks enable remote code execution, unauthorized access to databases, or full server takeover.

Insights from Wavestone's RedTeam

"Our operations increasingly succeed by targeting elements outside the core information system: Cloud/SaaS services, CI/CD platforms, IAM systems, etc."

"As was the case last year, 100% of RedTeam engagements uncovered passwords stored in shared spaces."

Backups remain a prime target...

As in previous years, most ransomware attacks also involved the compromise of backup systems, essential for any recovery. Securing backups continues to be a top priority for CIOs.

90%

of ransomware attacks managed by our CERT also compromised backups

Field insight: backups targeted before ransomware deployment

After gaining access, an attacker deleted the backups of a file server before downloading ransomware from a public repository.

The malware was executed on three Synology servers, resulting in data encryption, although one attempt failed on one of the servers.

... as well as business data compromise

Whether for espionage purposes or to pressure victims into paying a ransom, data theft remains one of the main impacts of cyberattacks. Monitoring and protecting business-critical data continues to present a major challenge for the future.

71%

of the incidents handled involved confirmed data theft

Field insight: business data exfiltrated to the dark web

An SQL injection on a web application allowed the attacker to deploy a web shell, granting direct access to internal systems.

The attacker then exfiltrated personal data from both the database and the file system, before publishing the sensitive information on the dark web.

Faster impacts after initial intrusion

The time between intrusion and impact continues to shrink, stretching detection and response capabilities. Organizations must now turn to greater automation, particularly through AI, to keep pace with this acceleration.

1,5 days

is the shortest time observed between intrusion and impact

Field insight: A lightning-fast ransomware attack

By exploiting a VPN still accessible with a default account, attackers were able to infiltrate the information system.

Then, in less than 24 hours, they gained control of a domain administrator account, exfiltrated sensitive data, and encrypted the information system and its backups.

Following the attack, the stolen data was published on the dark web.

Subsidiaries and partners used as entry points

Despite important progress within large organizations, less mature subsidiaries and third-party providers continue to offer significant entry points for attackers. Securing them at scale continues to be a major challenge.

56%

of attacks targeting large companies originated through subsidiaries or partners

Field insight: partner compromise leading to financial fraud

Following the phishing-based theft of a partner's account, the attacker gained access to their email and internal communications.

They then distributed fake bank account details (RIB) via email, using typo squatting to impersonate a legitimate client and divert payments.

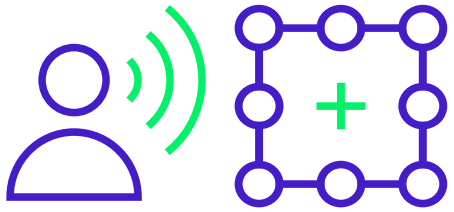
1 Evolutions of phishing

In 2025, attackers are combining innovation with social engineering to enhance the effectiveness of their campaigns.

Vishing

Fraudulent voice calls, sometimes enhanced with deepfakes, are becoming more frequent. Perceived as more authentic than emails, they often exploit urgency to deceive.
One such campaign targeted Salesforce users during the summer of 2025.

Finance, administrative, and IT support teams remain the most targeted.



Quishing

This emerging technique leverages malicious QR codes. Victims scan a code (e.g., placed over a legitimate sticker or on a fake document) that redirects them to a fraudulent site or content.

Quishing, especially in open environments, blurs user awareness and bypasses traditional filters.

Key recommendations

Raise awareness among employees and clients, who remain the first line of defense in the absence of reliable technical protection mechanisms.

Adapt internal processes to make attacks harder to execute: monitor privileged business accounts, strengthen helpdesk procedures, etc.

Enhance detection capabilities and ensure users and clients have a clear way to report suspicious activity or incidents.

2 Saas environments: the new attractive targets

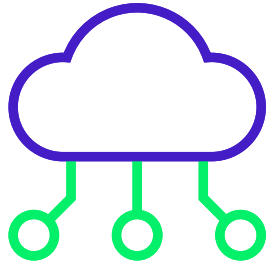
In 2025, collaborative applications and cloud services have become key entry points for attackers.

API compromise and abuse

Stolen credentials remain the primary entry vector into SaaS accounts.

Poorly secured APIs and third-party applications are also exploited to exfiltrate files and emails.

Once compromised, these platforms provide direct access to business-critical data.



Salesforce: A prime target

Recent attacks highlight the growing interest in CRM data.

Misconfigured APIs and account takeovers make Salesforce a target for both espionage and fraud.

Salesforce exemplifies the strategic value of SaaS CRMs for attackers.

Key recommendations

Enforce MFA or additional security measures on all sensitive SaaS accounts (business and IT).

Audit and regularly monitor exposed APIs and third-party integrations.

Continuously monitor access and detect unusual behavior in these environments.

3 Software supply chain poisoning

A persistent and complex risk to monitor.

Cryptocurrency theft via compromised open-source packages

In early September 2025, the compromise of 18 npm packages was disclosed. Malicious code had been injected into these widely used open-source components to enable cryptocurrency theft.

Unverified external code can quickly find its way into production environments.

Massive transformation of open-source packages into trojan horse

A few weeks later, a similar attack, known as Shai-Hulud, compromised over 500 npm packages. A worm spread by stealing maintainers' tokens and API keys, then injecting malicious code into other projects.

Shai-Hulud demonstrates how a single compromise can rapidly contaminate the entire open-source ecosystem.

Key recommendations

Map software dependencies and use Software Composition Analysis (SCA) tools.

Regularly verify and update third-party packages from trusted sources, and maintain your own internal repository.

Implement specific incident response plans for software supply chain attacks.

Supervise external developers with well-defined processes, strict access controls, and enhanced oversight.

4 AI-enhanced attacks becoming more sophisticated

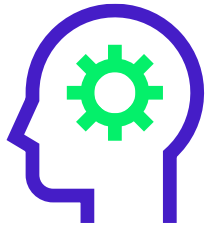
Requiring adaptation of defense mechanisms

Phishing & deepfakes

Phishing is evolving with massive, multilingual campaigns generated by AI.

Voice and visual deepfakes are designed to impersonate executives or IT support and can now be created very easily.

Phishing and deepfakes, amplified by AI, make it easier to deceive people.



Malware automation

Beyond development, AI is also used in the operation of malware.

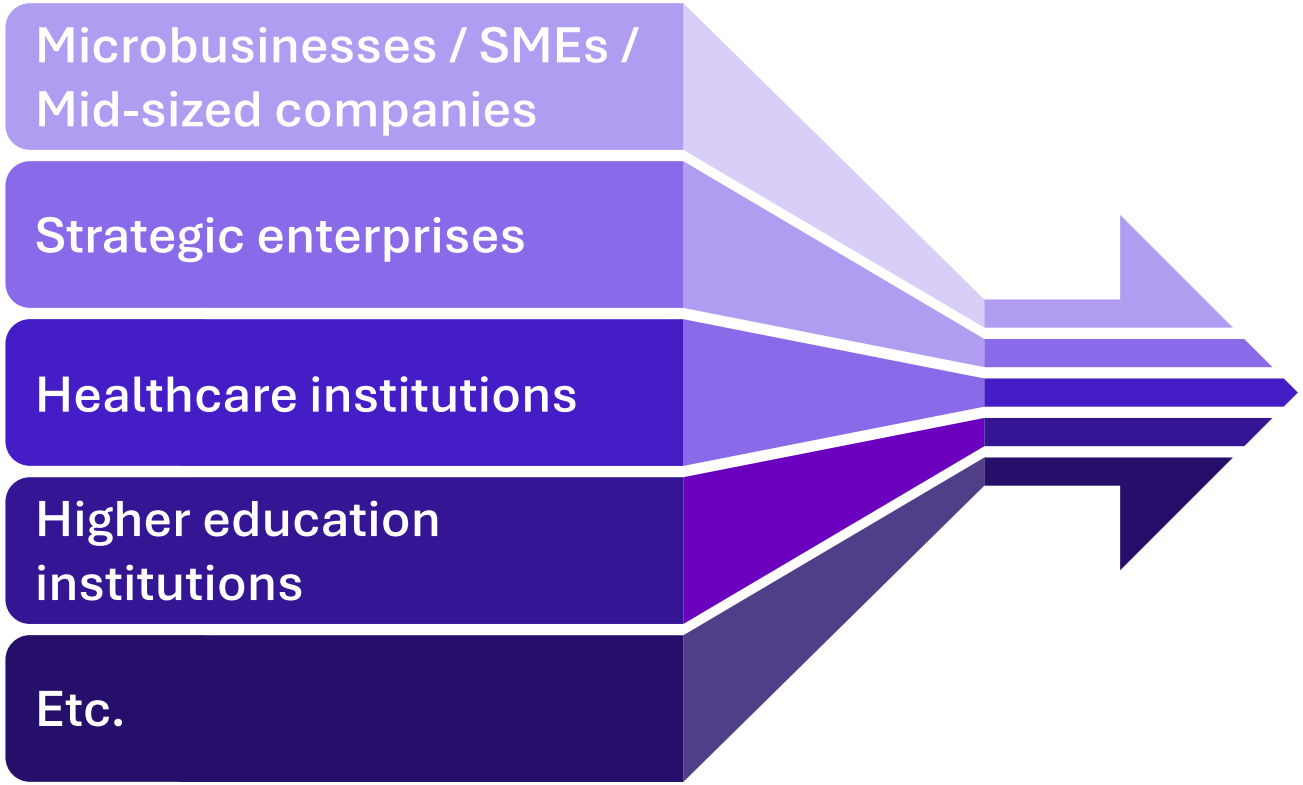
For example, PromptLock is a ransomware that automates its operations using generative AI: it can generate malicious scripts and decide whether to exfiltrate or encrypt data.

AI-powered malware is more scalable, personalized, and equipped with more advanced capabilities.

Key recommendations

- **Integrate deepfakes** into **crisis exercises and awareness training** to prepare teams.
- **Implement behavioral fraud detection** to ensure continuous monitoring.
- **Automate detection and response** to improve reactivity, notably by leveraging AI within SOCs.
- **Test the first anti-deepfake solutions**, as the market is beginning to offer mature options.

Attacks handled by CERT-Wavestone across all sectors and company sizes



21 major security incidents

More than 10 different sectors were supported by CERT-Wavestone this year, with the main ones corresponding to the key targets identified by ANSSI.

Whether in France or internationally, forensic investigations were required in every case.

Wavestone,

Leader in Cybersecurity

1,000 cybersecurity consultants combining functional, sector-specific, and technical expertise to deliver over 1,500 missions per year across around 20 countries (including France, the United Kingdom, the United States, Hong Kong, Switzerland, Belgium, Luxembourg, and Morocco).

Proven expertise from strategy to operational implementation:

- Risk management and cybersecurity strategy
- Digital compliance
- Next-generation cloud and security
- Penetration testing and security audits
- Incident response and crisis management
- Digital identity (for users and customers)

Experience across numerous domains, notably in financial services, Industry 4.0, IoT, and consumer goods.

Contact our experts

Gérôme BILLOIS
Cybersecurity Partner
gerome.billois@wavestone.com

Quentin PERCEVAL
Head of CERT-Wavestone
quentin.perceval@wavestone.com