



2024 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



Worldwide

presence



+5 500

employees



943,8 M€

pro forma revenue



Independent

perspective & solution-based actions



Who are we?

CERT-Wavestone: 40 experts specialized in cyber crisis

During incidents...

- / Investigations and forensics analysis
System, network and code analysis
- / Crisis management
Steering, anticipation, support for internal and external communication, support for regulatory requirements
- / Defense strategies
- / Remediation and reconstruction
- / Threats identification

...and upstream

- / Crisis exercises
- / CSIRT training and reinforcement
- / Cyber attack simulation
RedTeam / Purple-team
- / SOC and CSIRT evolution
Maturity assessment, training, action plan
- / Phishing campaign
- / Cyber resilience assessment
- / Internet footprint assessment
- / Cyber Threat Intelligence



Wavestone was the first company to receive and renew its "**Prestataire de Réponse aux Incidents de Sécurité (PRIS)**" certification from ANSSI for all areas:

- / Indicator of Compromise Search [REC]
- / Digital and Forensics Investigation on Limited Perimeter [IPR]
- / Digital and Forensics Investigation on Extended Perimeter [ILP]

This report is an analysis of the 20 major incidents handled by the CERT-Wavestone between August 2023 and September 2024.

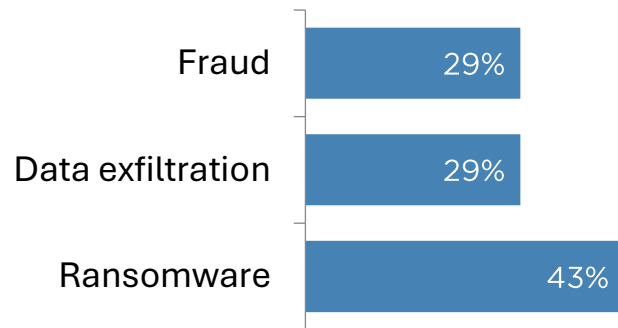
What are the attackers' motivations?

Financial gain remains the main motivation of attackers, and ransomware dominates

Financial gain (50%)

Mainly through the blocking of information systems, the threat of stolen information disclosure or persistent fraud.

46% in 2023, 51% in 2022



Espionage (10%)

These attacks are increasing notably due to a tense geopolitical context.

8% in 2023, 0% in 2022

Internal malice (5%)

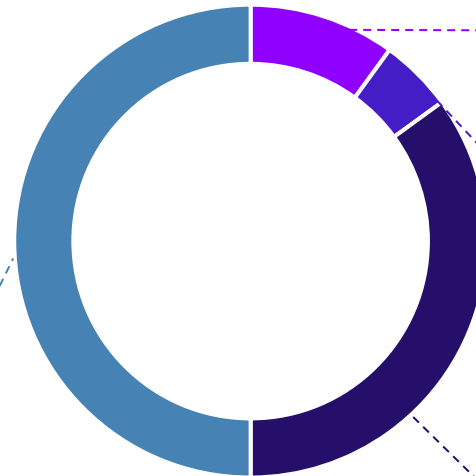
With the aim to steal internal data in most cases, notably when employees leave the company.

6% in 2023, 29% in 2022

Undetermined (35%)

The attacker's motivation remain unknown (no impact, attack interrupted, etc.).

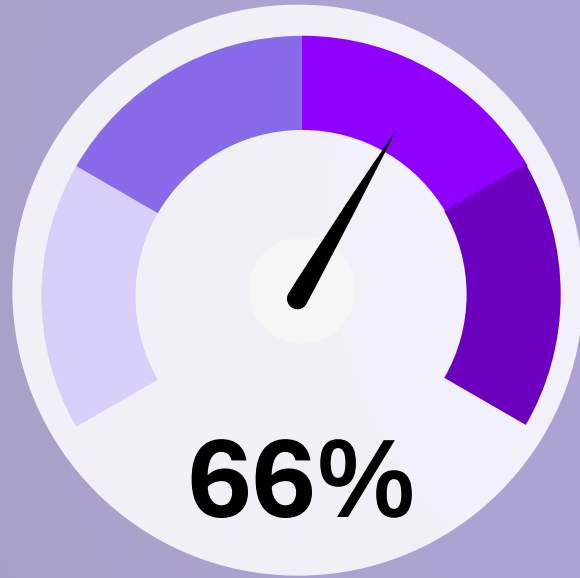
29% in 2023, 16% in 2022



Who are the attackers' targets?

Large companies targeted notably through their main subsidiaries or partners

The cybersecurity progress of major corporations protect them against the most common threats, but their less mature subsidiaries remain vulnerable.



of attacks on large companies targeted their subsidiaries.

Feedbacks from the field: a ransomware attack on a subsidiary

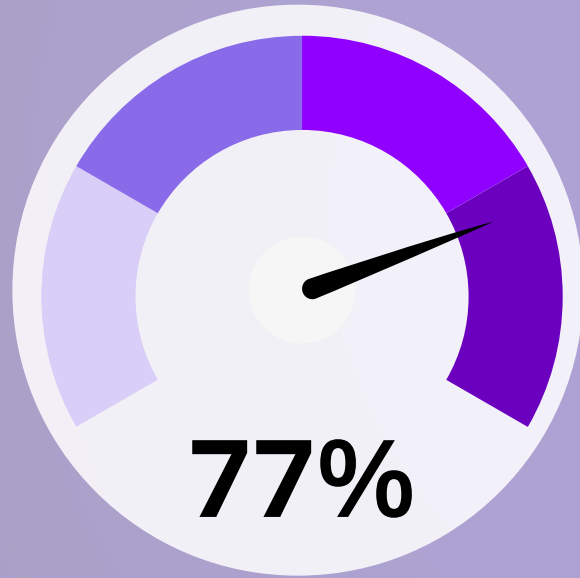
A subsidiary of a **banking and insurance group** was attacked through a critical vulnerability in a **component exposed to the Internet** and not kept up to date.

Then, the attacker took advantage of permissive filtering rules to **propagate within the information system, extract data** and launch a ransomware.

Who are the attackers' targets?

Compromise of **business data**: a prime objective for the attackers

Whether for espionage or to encourage the payment of a ransom, data theft remains one of the main impacts of cyber-attacks.



*of attacks involved
a confirmed data theft.*

Feedbacks from the field: 2 years of business data espionage

An attacker maintained a persistent access to the information system of an **industrial** company during 2 years.

He notably exfiltrated emails at regular intervals.

Its presence was only revealed when a phishing campaign was carried out from one of the compromised addresses.

Who are the attackers' targets?

Companies' **vigilance** and **responsiveness** challenged by attackers

As attacks are becoming increasingly fast, detection and response capabilities of SOCs and CERTs are key to efficiently counter cyber-attacks.



between the intrusion and the impact of an attack (shortest delay observed).

Feedbacks from the field: a ransomware attack in the twinkling of an eye

An attacker performed a brute force attack to gain access to a local VPN gateway account.

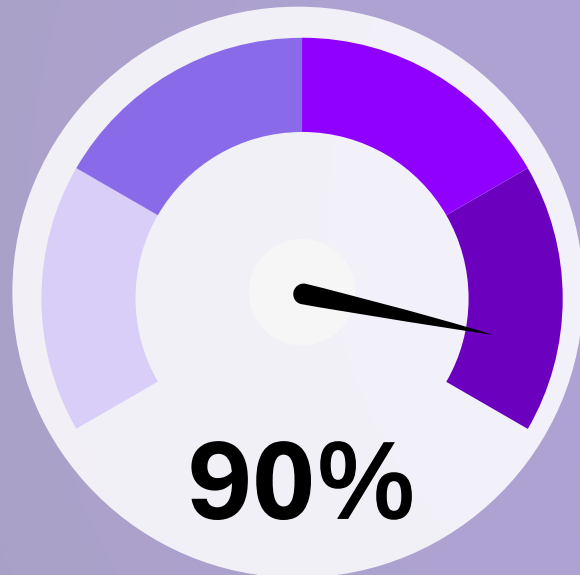
In less than 2 hours, he elevated his privileges and compromised the Active Directory domain through service accounts.

Over the next 2 days, the attacker exfiltrated massive amounts of data and then launched his ransomware attack over the weekend.

Who are the attackers' targets?

Backups: a prime target for attackers to prevent the rebuild of the IS

Deleting backups is an increasingly common objective for attackers to position the payment of the ransom as the only option for the victims.



of ransomware attacks have directly or indirectly targeted backups.

Feedbacks from the field: compromised backups to prevent IS rebuild

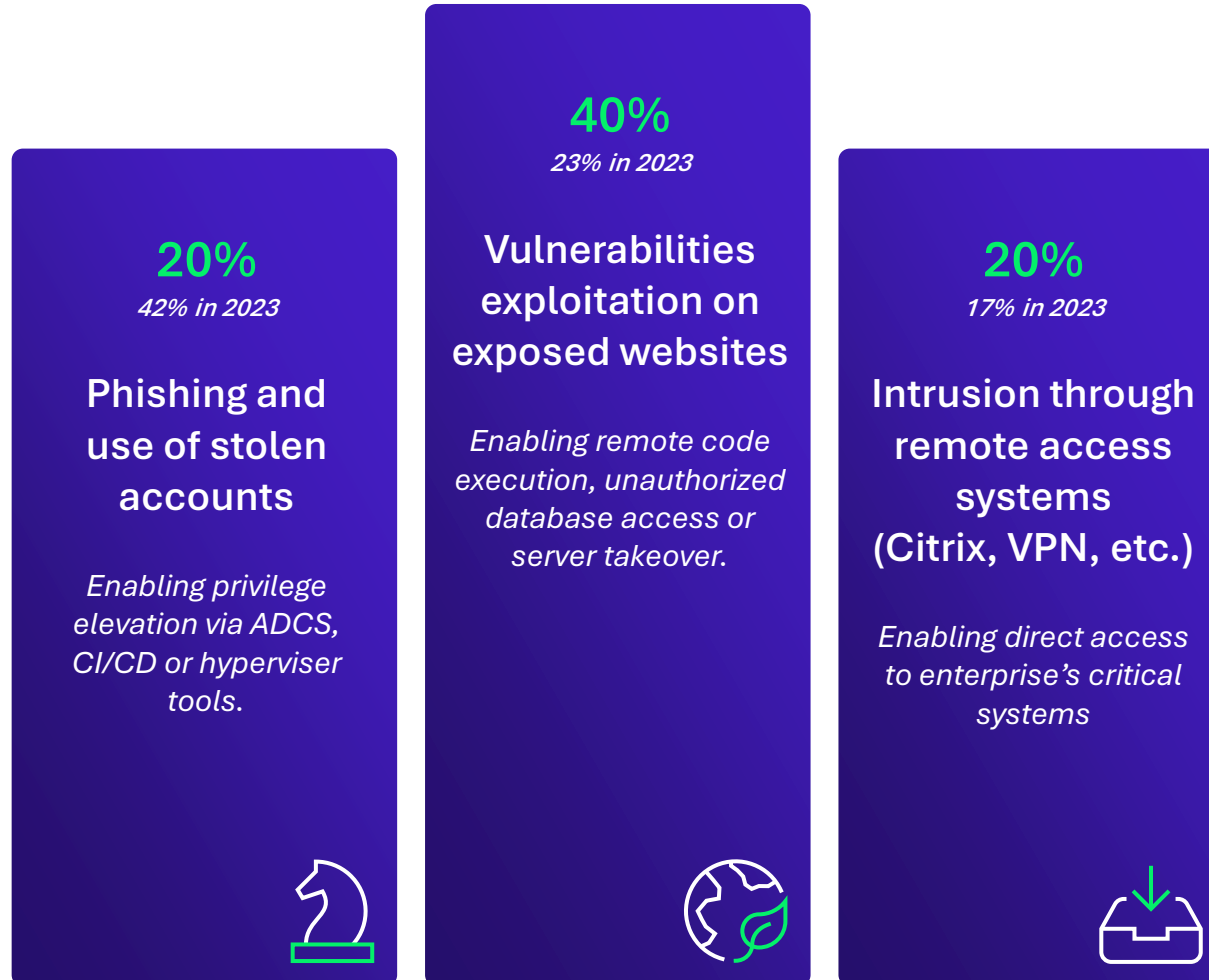
In the healthcare sector, an attacker became administrator of the Active Directory.

He then **disabled the creation of new backups, and deactivated the alert system** monitoring their creation.

Finally, the attacker **waited around ten days** before launching his ransomware attack, thus ensuring that the victim had no recent backup to rebuild.

How do they get in?

Vulnerabilities of exposed websites, the first entry point to the IS



Verbatims from Wavestone RedTeam

"100% of RedTeam engagements have found passwords stored in shared folders."

"Our RedTeam experts are able to deploy an automated vulnerability exploitation tool a few days after a CVE is published."

What major threats can we anticipate in the years ahead?

Artificial Intelligence, a new **weapon** available for the **cybercriminals**

Malicious script generation

AI enables to generate malicious scripts that **facilitate the identification of vulnerabilities** and **the execution of attacks** by actors with a lower level of expertise.

Thanks to an AI, Google has recently discovered an unknown vulnerability in the source code of SQLite.

HP Researchers highly suspect the use of AI to develop the malicious code launching the download of AsyncRAT malware.



Phishing

AI increase phishing capabilities by **automating and improving** these attacks, making them even more realistic.

According to Proofpoint, phishing attempts have increased by ~30% in Japan, Korea and United Arab Emirates since the introduction of ChatGPT.

Deepfake

AI facilitates identity theft (and in particular president scams) **through fake audios or videos**

In Hong Kong, an employee was tricked by a Deepfake during a video conference, costing the company 26 million dollars.

What major threats can we anticipate in the years ahead?

Artificial Intelligence, an opportunity for new and unfamiliar attacks

Poisoning

.....
The attacker manipulates training data to **compromise the integrity of the AI model.**

More than 100 poisonous models are available on the Hugging Face platform¹

Oracle

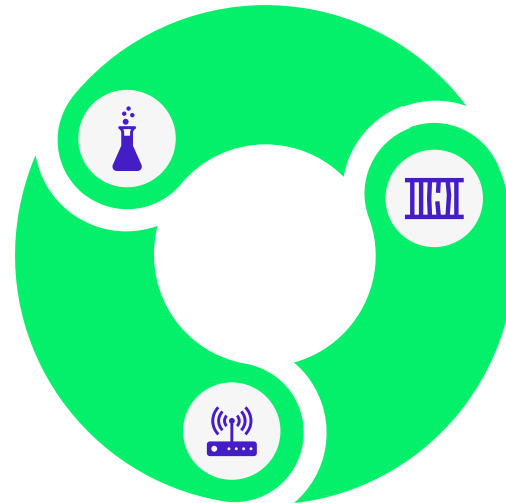
.....
By interacting with the AI model, the attacker attempts to **extract information** about the training data or the AI model itself.

Dozens of projects to transform Copilot into "Copirate" are available on Github²

Evasion

.....
Evasion attacks involve the careful modification of input data **to lead the model to erroneous decisions.**

Several dozen of prompt injection tools for this type of attack are available on GitHub




Development environments for AI tools, like data tools, are also exposed to standard attacks because best security practices are not always applied.

¹Platform for providing AI models


²Source : "Microsoft Copilot: From Prompt Injection to Exfiltration of Personal Information"

Companies must invest in the measures with the greatest impact to protect them against cyber-attacks




Identity management

- Control privileged account management from end-to-end (PAM)
- Secure identity repositories in the same extent as the most critical assets



Monitoring


- Ensure a complete coverage of the assets (EDR)
- Set up a governance to ensure appropriate responsiveness
- Manage vulnerabilities across the entire IS



Backup


- Secure and monitor backup systems
- Isolate backups from the Active Directory
- Make offline or immutable copies of backups

... without forgetting the least managed perimeters




Subsidiaries

- Audit and control subsidiaries' cyber maturity level
- Manage all interconnections with subsidiaries
- Implement a "Red Button" process to isolate subsidiaries



Cloud

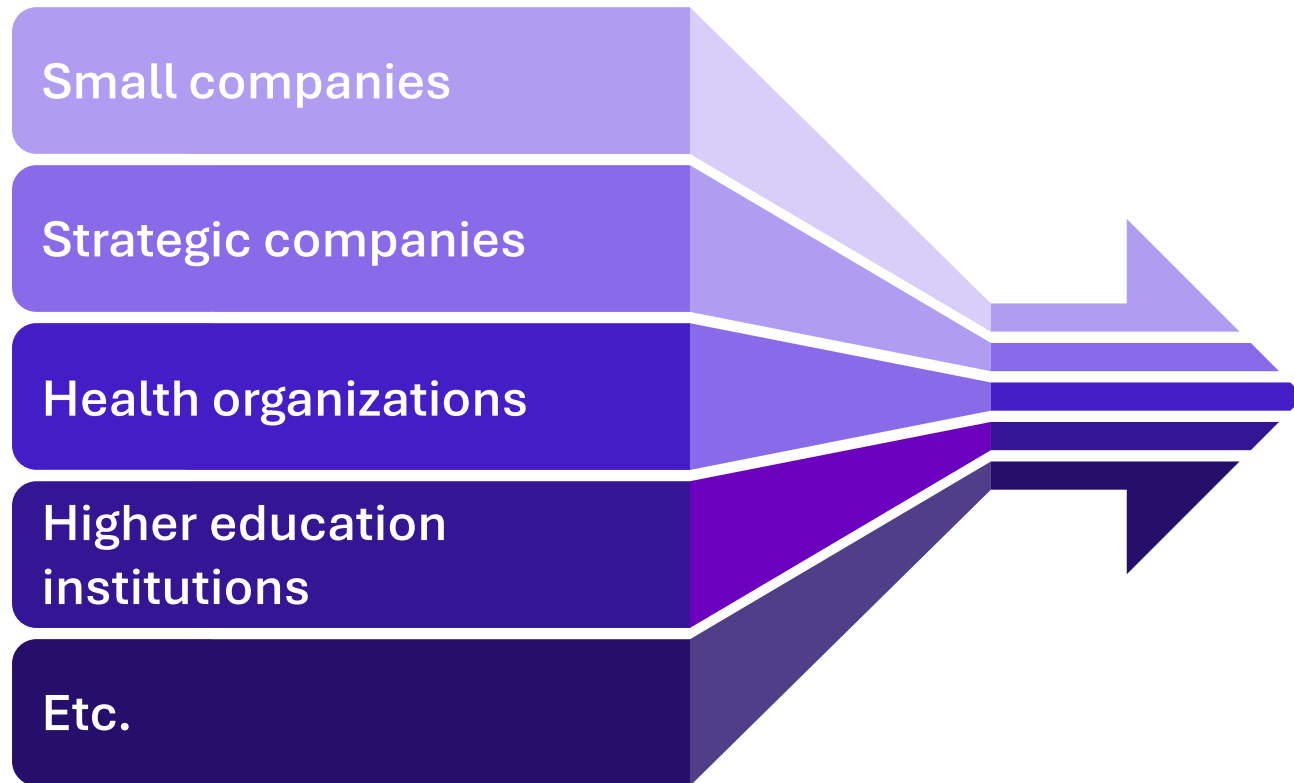
- Clarify cloud operating models
- Apply systematically the principle of least privilege
- Control automatically the implementation of hardening



AI

- Secure AI development environments
- Conduct crisis management exercises using AI scenarios
- Set up an AI investigation team

Attacks managed by the CERT-Wavestone across all sectors and company sizes



20 major cybersecurity incidents

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

Whether in France or abroad, forensic investigations have been systematically necessary.

Wavestone,

Leader in cybersecurity and operational resilience

1 000 cybersecurity consultants who combine functional, sectoral and technical expertise to cover more than 1 000 assignments per year in 20 countries (including France, UK, USA, Hong Kong, Switzerland, Belgium, Luxembourg and Morocco).

A proven expertise from strategy to operational implementation:

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

An experience in a wide range of fields, including financial services, industry 4.0, IoT and consumer goods

Contact our experts



Gérôme BILLOIS
Cybersecurity Partner
gerome.billois@wavestone.com
+33 (0)6 10 99 00 60
✉ @gbillois



Quentin PERCEVAL
Head of CERT-Wavestone
quentin.perceval@wavestone.com
+33 (0)7 64 47 21 36