CERT-W 2023 Report

Trends and analysis of one year of incident response

By the CERT-Wavestone

September 2023

The Positive Way
WAVESTONE

Wavestone

We support large companies and organizations in their most critical transformations

530 M€

~ 4 500
employees

15 offices
in 9 countries

Business
Technology
Sustainability

Who are we?

Wavestone CERT-W

40 cyber crisis experts

During cyber incidents...

- **Forensics investigations**
  Systems analysis, network and code analysis
- **Crisis management**
  Steering, anticipation, support for internal and external communication, supporting regulatory compliance
- **Cyber Defense**
- **Remediation & reconstruction**
- **Threat Hunting**

...and before them

- **Crisis drills**
- **Cyber attacks simulation**
  Red-team / Purple-team
- **SOC and CERT processes definition, maturity assessment, trainings**
- **Cyber Watch & Threat Intelligence**
- **Cyber resilience assessment**
- **Technical analysis of cyber attacks**

Wavestone is one of four companies qualified as a "**Security Incident Response Service Provider**" (PRIS) by ANSSI.

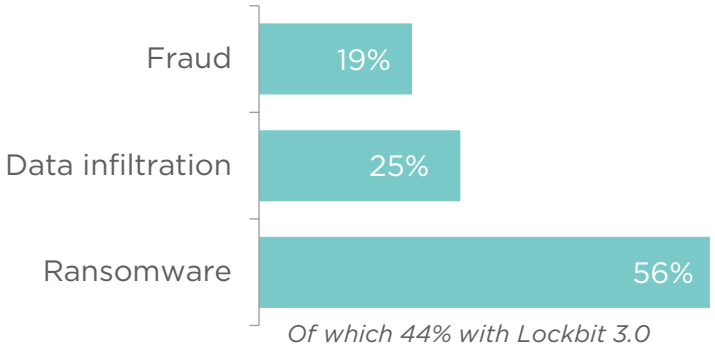
What are the attackers' motivations?

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

Financial gains (46%)

Financial gain may be obtained through ransom to block IS and/or non-disclosure, or by reselling stolen data.
Cases of fraud have reappeared this year.

51% in 2022

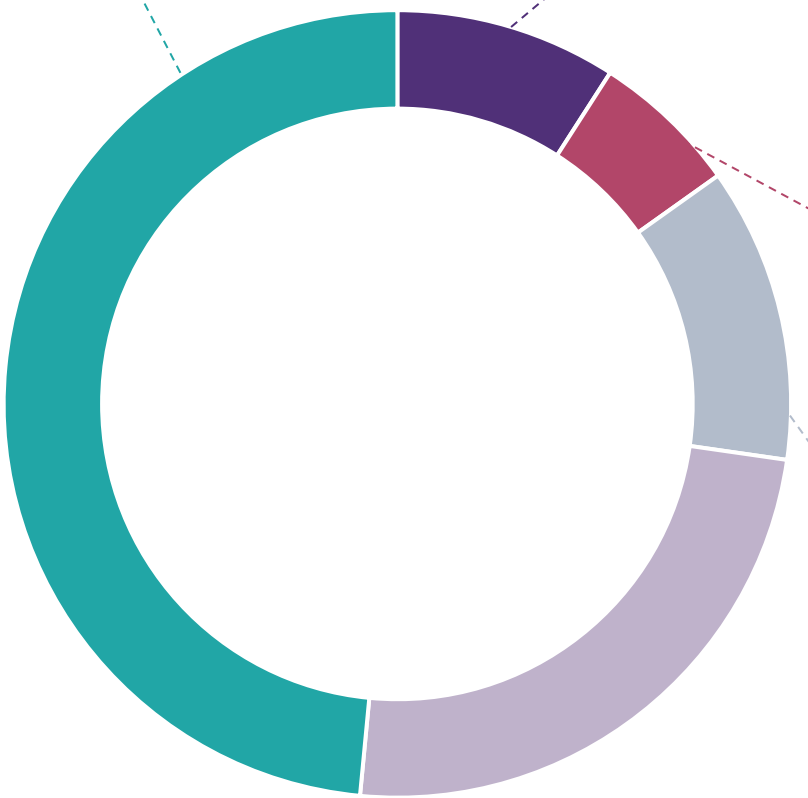


Of which 44% with Lockbit 3.0

Undetermined (29%)

Despite confirming compromise, the attacker's motives could not be identified (attack stopped before impact, systems compromised without action, insignificant impact, etc.)

16% in 2022



Malicious (6%)

With most cases involving internal malicious activity aimed at deleting data, external actors also carry out defacement attacks.

9% in 2022

Espionage (9%)

Not previously identified in our assistance, attacks of this kind are a consequence of the tense geopolitical landscape.

0% in 2022

Preparation for the next cyber attack (11%)

Misappropriation of information or resources to carry out an attack on another target (spam/phishing, Office 365 compromise, physical intrusion etc.)

32% in 2022

Which targets?

Attacks remain opportunistic

While all sectors and all company sizes are targeted, four trends are confirmed:

Smaller structures affected	Data is more targeted	Increasingly rapid and multiple attacks	Leverage through infrastructure
Large companies have improved their **detection and response capabilities** in recent years and are less affected by attacks	**77%** of observed **ransomware** cases **combine encryption and data exfiltration,** with the ransom note almost always mentioning data theft	**The execution time** of a **ransomware** attack has **dramatically reduced**, from several weeks to a few days	**Virtualization environments or platforms** such as ESXi have become a prime target for attackers
In response, cybercriminals are focusing on **more simple targets** with less mature cybersecurity skills	The threat of publication of stolen data has become the attackers' **most effective pressure tactic**	**Attacks involving multiple ransomwares** are emerging, targeting the same victim within days of each other	These platforms can affect several hundred or even thousands of virtual servers in **a single attack**

What are the attackers' motivations?

Using stolen accounts is still the main entry point for attackers

On-premise Active Directory infrastructure are still key targets for attackers and were involved in **1 in 2 cyber crises managed** by CERT-W during the 2022-23 period.

Trends of 2023

Compromise of Office 365 accounts

which have become the standard office solution in companies

facilitated by the absence of multi-factor authentication (MFA)

Why are large companies less affected?

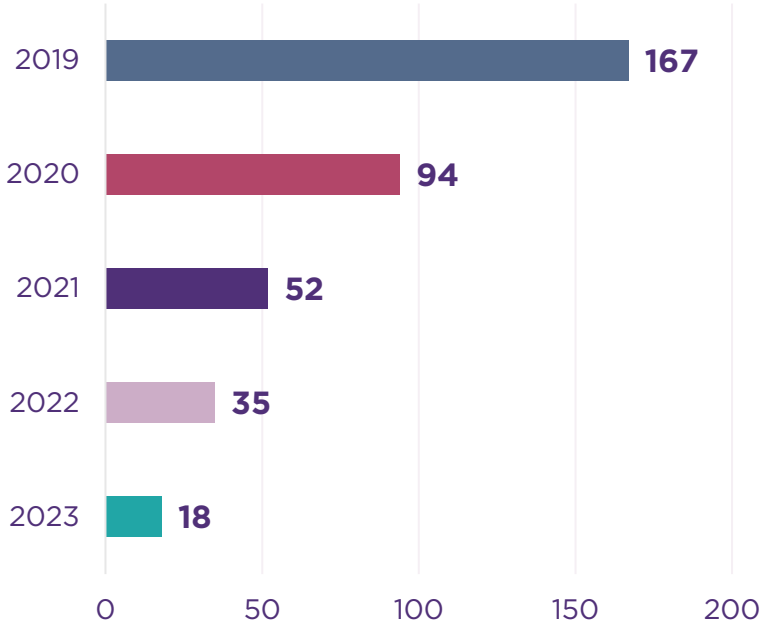
Investment in cybersecurity by large organizations pays off

Shorter detection times, more effective cybersecurity tools, increased response capabilities...

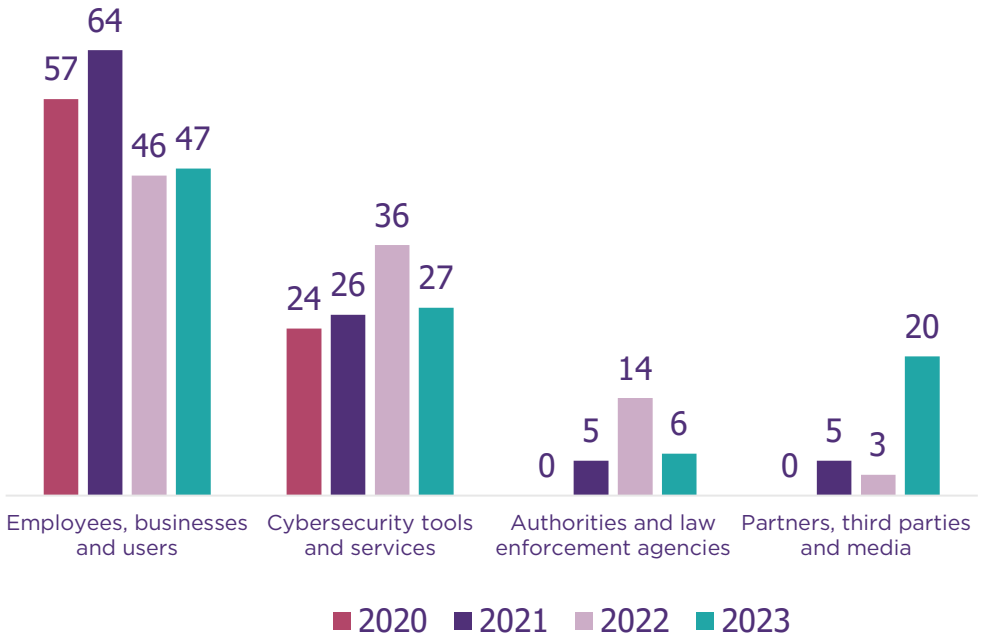
Delay between initial intrusion and detection

18 days

Compared with **71 days** on average for small and medium-sized companies



Distribution by security incident detection source



Benchmark CERT - 2023

New emergency situations: IS decoupling in the face of a third-party threat

Isolate a geographical perimeter
In a tense geopolitical context

Isolate a business unit or function
In case of compromise or fear about a specific IS

Triggering crisis management to ensure a first level of decoupling within a few days

Protect the core business (*Minimal Viable Company*)

Identify vital business processes in critical applications

Segregate networks

To authorize only strictly necessary communications

Increase the level of surveillance

To be able to identify and block any attempt of malicious action

Investigate proactively

To search for traces of compromise before or after the hostile perimeter takeover

Which strategy to adopt?

Quick carve-out: Save time to protect yourself, but expose yourself to **espionage risks**

VS

IS isolation: Protect quickly, but expose yourself to **risks of retaliation**

(cyber attack, legal action, etc.)

What major threats can we anticipate in the years ahead?

Generative Artificial Intelligence,
New capabilities for cybercriminals...

IA SOLUTION MISAPPROPRIATION

Drafting fraudulent documents, designing malware, injecting messages, etc.

NEW TOOLS

Automating attacks, adapting existing malware, etc.

USE OF DEEPFAKE

Personalized phishing, identity theft by voice imitation or image hijacking, etc.

... But also new targets, vulnerable to innovative attacks

ChatBot for online sales

Anti-fraud systems

Detection systems

Automated decision

Infection attacks

/ Dataset poisoning
/ During AI training and retraining

Manipulation attacks

/ Evasion
/ Model reprogramming
/ Denial of service

Extraction attacks

/ Membership interference
/ Model inversion
/ Model extraction

Companies must continue to invest to defend themselves against new attacks

What you can do to prepare yourself against future threats...

Identify and be ready to protect the core business (Minimum Viable Company): map **vital business processes** within critical applications, deploy appropriate protection measures, and be able to isolate and rapidly rebuild them.

Increase the level of attention to new risks linked to the use of AI, **assess the security of internal AI systems**, **raise employee awareness** and review business processes that could be impacted (fraud detection, etc.).

Olympic Games - Paris 2024

Anticipate any cyber-attacks that could indirectly target the event, its partners or the public (e.g., fraud)

Ensure the availability of teams and cyber partners, bearing in mind that the event will be held in the middle of the summer season

...without forgetting best practices!

Define a Data Loss Prevention strategy and **adopt a proactive attitude** to the threat of exfiltration of business and infrastructure data (e.g., Active Directory database)

Deploy **multi-factor authentication** (MFA) on all environments exposed to the Internet, including **Office 365 environments**

Protect the infrastructures that support your core business (partitioning, monitoring vulnerabilities and security patches, rights management, etc.), **including in the case of virtualization and in the cloud**

Financial motivation prevails, threatening smaller organizations

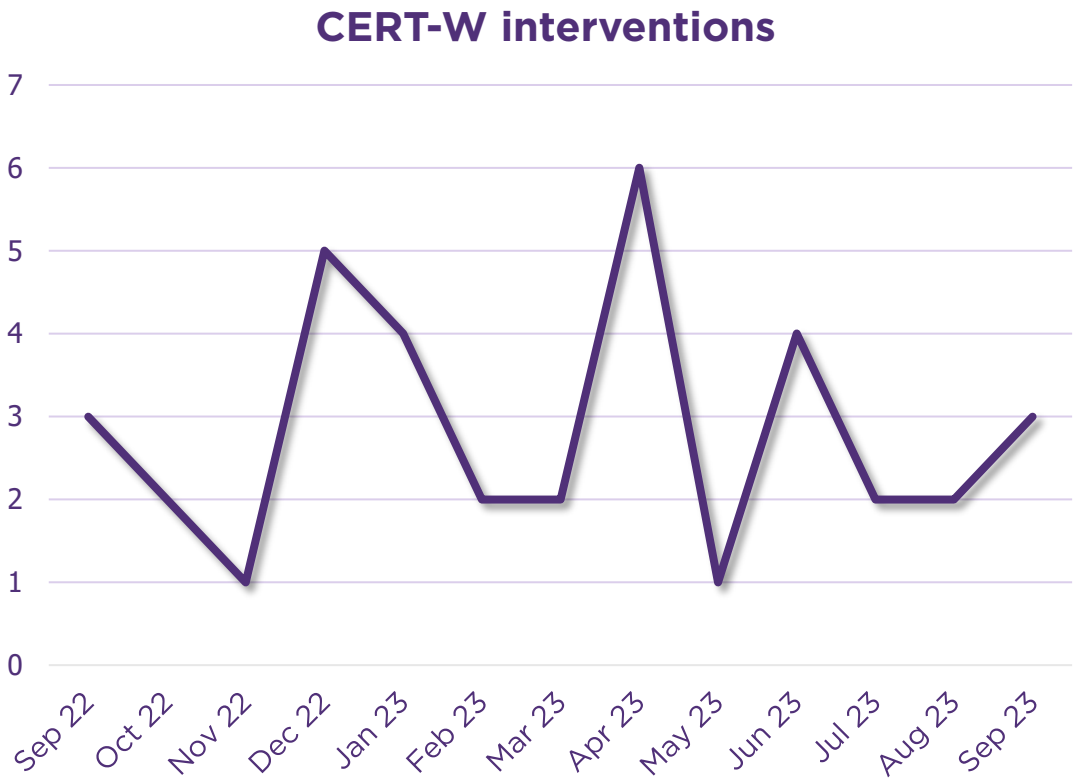
Financial gain remains the primary motivation for attackers.
The methods of intrusion remain the same, mainly using valid, often unsecured accounts

The threat is **still largely opportunistic.**
As larger companies are better prepared, **the threat is shifting to the small and medium-sized business market.**

Criminal organizations are becoming increasingly organized and industrialized. In the current geopolitical context, these structures are becoming more radical, motivated by destabilization.

Investment is paying off for large companies, which must **continue their investments, trainings and raising awareness among their employees** to defend themselves against future threats.

Summary of cyber attacks managed by CERT-W



CERT

This study was based on cyber incidents and crises handled by the CERT-W team between the months of September 2022 and September 2023 (included).

37 major cyber security incidents

in **large companies or public organizations** were dealt with by CERT-W this year.

For each case, **forensic investigations** were required and **direct impacts** on the information system were observed.

These included **16 cyber crises** where the advanced compromise of the information system required a **dedicated crisis organization.**

Wavestone, leader in cybersecurity

Wavestone's 900 cybersecurity consultants combine functional, sectoral and technical expertise to cover over 1,000 assignments a year in some 20 countries (including France, the UK, the United States, Hong Kong, Switzerland, Belgium, Luxembourg and Morocco).

Proven expertise from strategy to operational implementation:

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

Particularly in financial services, industry 4.0, IoT and consumer goods.

Our experts

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

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