Cyberattacks in 2021:
Ransomware, still threat n°1

By the CERT-Wavestone

October 2021

Wavestone

We support large companies and organizations in their most critical transformations

Business & Technology

13 offices
in 8 countries

CA
418 M€

+3 000
Employees

CERT-Wavestone :
40 cyber crisis experts

24/7 during an attack...

- **Digital Investigation / Forensics**
  System, network, malicious code scans
- **Cyber and business crisis management**
  Steering, anticipation, support for internal and external communication, support for regulatory notifications
- **Defence of the IS**
- **Remediation & Reconstruction**
- **Threat Hunting**

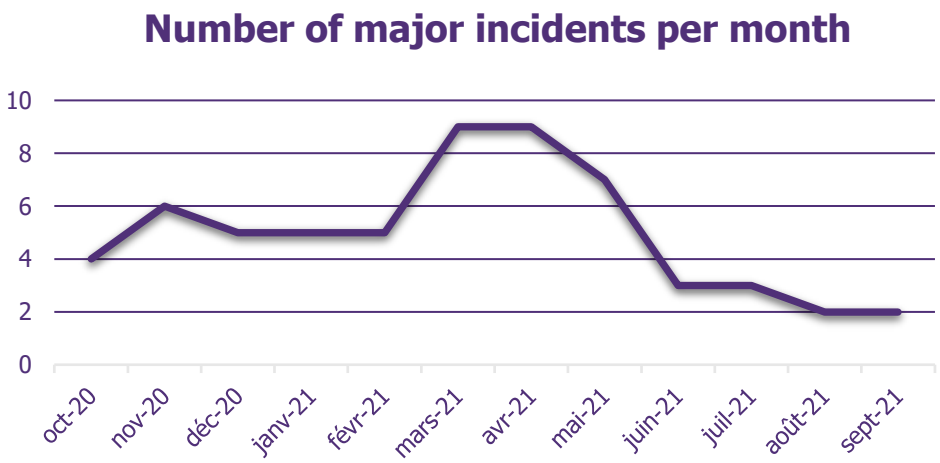
... but also upstream

- **Organization of crisis exercises**
- **Simulation of cyber attacks**
  red-team / purple-team
- **CERT and SOC Definition, animation and training**
- **Cybercrime monitoring**
  Watch & Learn
- **Assessment of the attractiveness of the company**
- **Analysis and decryption of attacks**

Wavestone is the first company to obtain the Security Incident Response Provider (PRIS) qualification by ANSSI.

Qualification N°1443 | Duration of 3 years from 29/06/2020

Assessment of cyberattacks managed by CERT-W



A significant drop-in activity between June and September 2021

CERT

A study based on the interventions of Wavestone's Security **Incident Response** Team between October 2020 and September 2021

60 major security incidents

(+15% volume in number of days vs 2020)

that led to the interruption of business activities or an advanced compromise of the IS, including 17 crisis requiring a specific organizational system

Security Incident Response Benchmark

A DESIRE TO SHED LIGHT ON AND SHOW THE EVOLUTION OF THE STATE OF THE CYBER THREATS, WHILE ALSO PROVIDING THE KEYS FOR BETTER ANTICIPATION AND REACTION

Who are the attackers and what are their motivations?

How did they get into the systems?

When and how have they been discovered?

How long does a major crisis last?

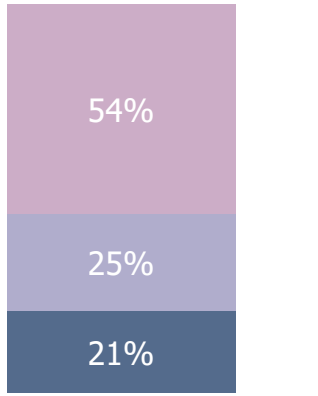
How to be prepared to limit the impacts?

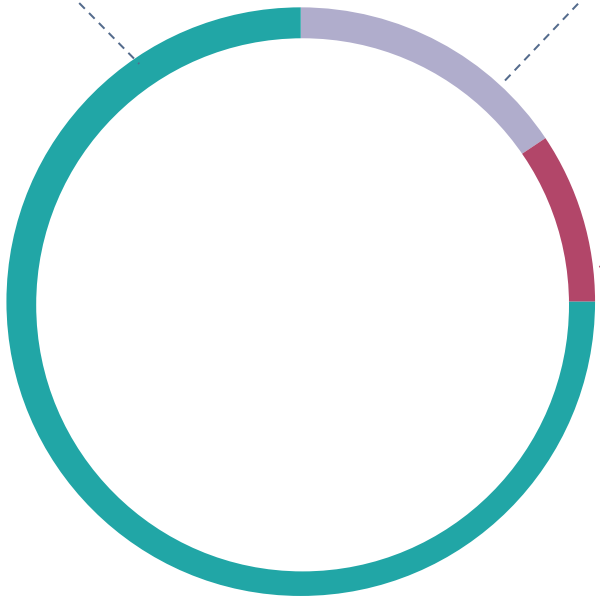
Financial gain remains the first motivation of attackers

DISTRIBUTION OF SECURITY INCIDENTS BY ATTACKER MOTIVATION

Financial gains (75%)

Financial gains can be obtained through ransoms to unlock the IS, from blackmail to non-disclosure of data or by reselling stolen data





Undetermined (15%)

Despite the compromise, the attacker's motivations could not be identified (attack abandoned, interrupted, compromise of systems without subsequent actions...)

Gains in attack capability (10%)

Misappropriation of information or resources to carry out an attack on another target (spam/phishing, DDoS, supply chain...)

Benchmark
CERT - 2021

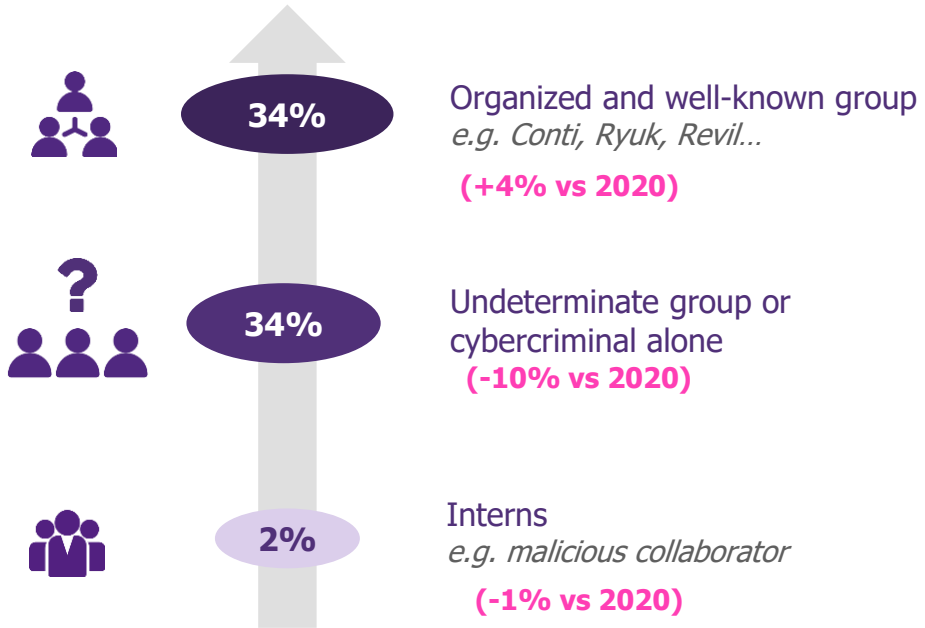
Largely opportunistic attacks by organized groups

What types of threats?

57%

attacks are opportunistic, attacks that do not target a particular organization.

Which attacker profiles?



In **30% of cases (+8% vs 2020)** it was not possible to determine the profile, usually due to a lack of data to analyze.

Benchmark
CERT - 2021

Always the same gateways to break into the systems

20%
Fraudulent email to steal 1st information or trap a computer (phishing…)

-5% vs 2020

23%
Using valid accounts to enter the IS (password theft, reuse…)

+5% vs 2020

18%
Remote access service using security vulnerabilities or configuration flaws
(Citrix, VPN…)

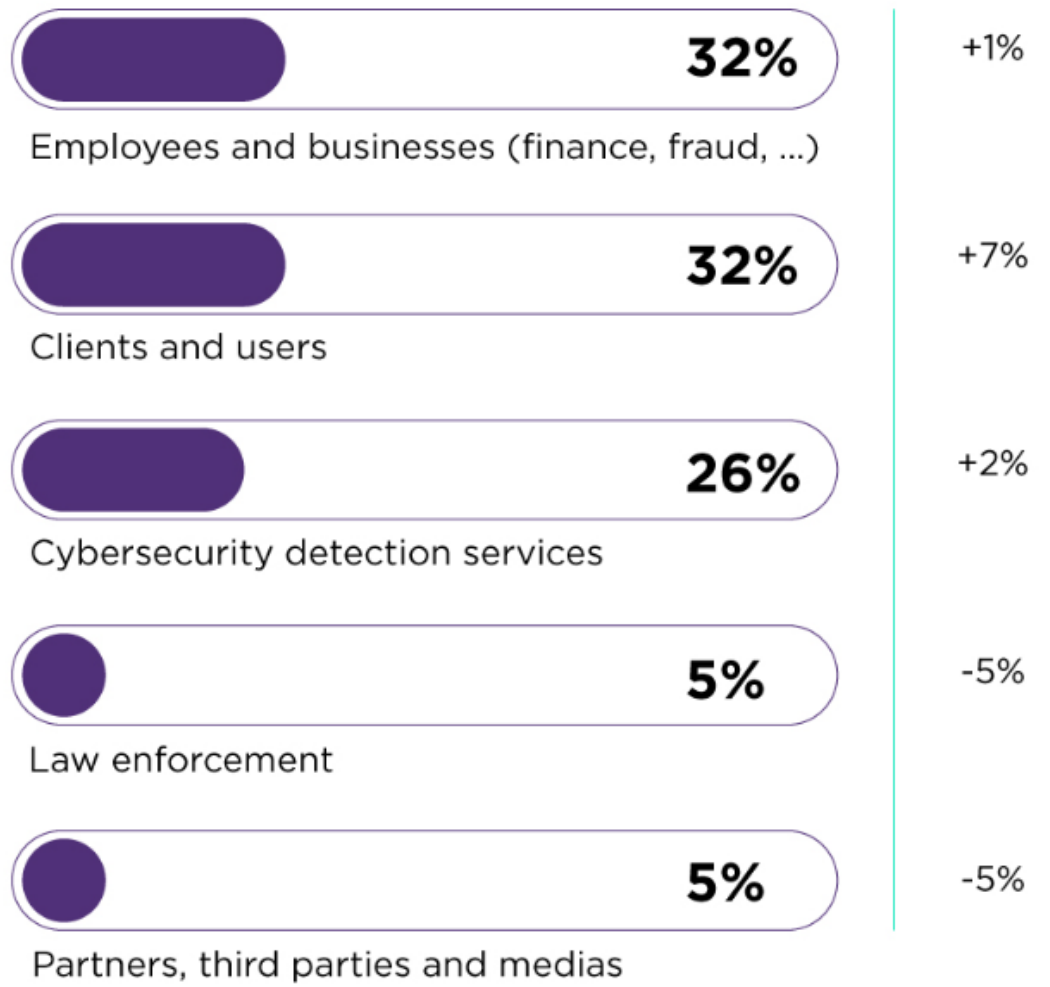
+2% vs 2020

Benchmark
CERT - 2021

Only **26% of major incidents** were identified by enterprise detection services

In **5% of cases,** Wavestone was able to stop the attack before its final impact.

Distribution by source of detection of security incidents

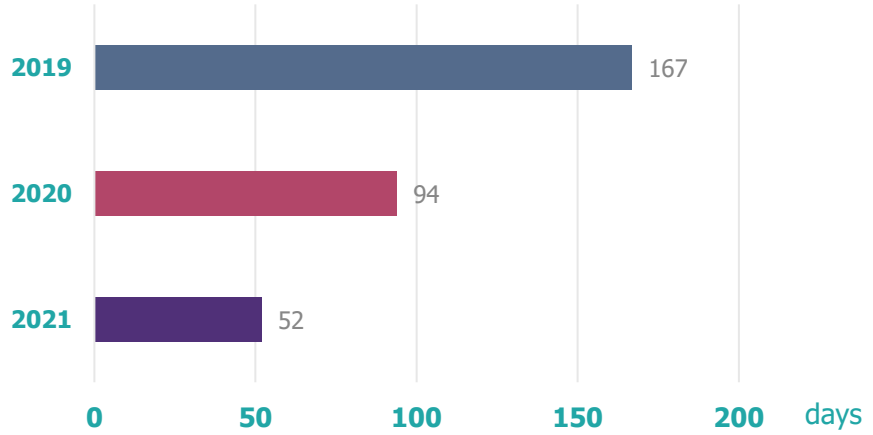


Benchmark
CERT - 2021

Almost half the average time elapsed between an intrusion and its detection

52 days

Average time elapsed between an intrusion and its detection **compared to 94 days (-45%) in 2020**



Benchmark
CERT - 2021

Ransomware: the most frequent and impactful type of attack

60% of incidents are caused by a ransomware attack (89% of managed crisis are ransomware)

1/3 ransomware attacks combine data theft and IS locking

In **90%** ransomware attacks, data has been irretrievably lost

In **21%** of ransomware attacks, backup systems have been targeted, until they are made unusable

GO FASTER

Increasingly quicker attackers

3

days only between initial access and ransomware deployment for the fastest attack
(25 days on average)

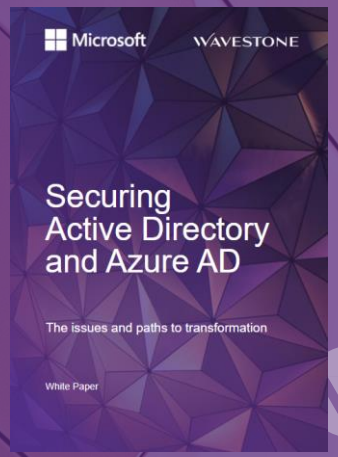
A common denominator of all ransomwares managed by CERT-W

A compromised ACTIVE DIRECTORY

The attacker had domain administration accounts in...

100% of crisis

To go further:
Check out our Microsoft/Wavestone white paper on securing Active Directory and Azure AD



Benchmark
CERT - 2021

Large-scale ransomware crises:

HARD DEADLINES... BUT IMPROVING

2
days
to mobilize the crisis at a cruising pace

2
Weeks
to recover a business situation in degraded operation

2
month
for a complete return to normal

Benchmark
CERT - 2021

60
people on average

250
maximum people

10
providers in reinforcement on average

Less paid ransoms?

The number of ransoms varies...

Ransoms fluctuate between

100.000 €

and

2.000.000 €

depending on the scale of the attack and the size of the company

Less than

5%

of victims paid the ransom.

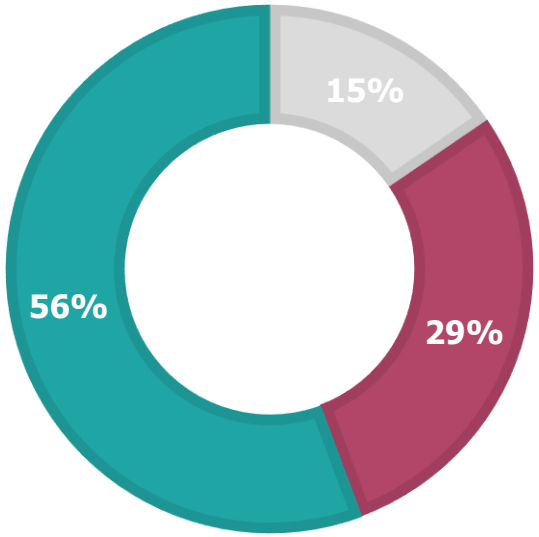
(Vs 20% in 2020)

... but their payment is infrequent

The payment of the ransom does not in any way accelerate the time of resolution of the crisis.

Benchmark
CERT - 2021

56% of major incidents were not anticipated by victims



- Solicitation of CERT-W via cyber insurance contract
- CERT-W subscription contract
- No incident response partner

42 %

of victims had not conducted a cyber resilience project (crisis exercise, backup security, reconstruction tests...)

Most victims did **not have an incident response partner** before the attack

Benchmark CERT - 2021

Prevent your business from being an easy target

TOP 5

ACTIONS TO PREPARE FOR AN ATTACK

Protect the most critical assets adopting security best practices (security patches, rights management, administrator management...)

Improve the efficiency of attack detection with a specialized service (24/7 surveillance, detection perimeter adapted to the threat, EDR...)

Know how to manage a major crisis (24/7 team, specific means of communication...) by prioritizing crisis exercises on various scenarios (IS blocking, targeted data theft, massive data theft...)

Strengthen backup security (hardening, access rights, insulation...) and train to rebuild urgently (procedures, specific equipment...)

Take out cyber insurance and a contract with a specialized team (surround themselves with experts who can speed up the resolution of the incident)

Want to know your degree of resistance?
Evaluate yourself using the W-CyberBenchmark

In case of emergency for investigations or crisis management

Contact CERT-W cert@wavestone.com

Attacks still on the rise with ever stronger impacts

Number of major incidents processed by Wavestone increased in volume in the year (+15%).
The motivation for financial gains remains in the majority (75%).

Ransomware is **the number 1 threat.**
The combination of IS **freezing and data theft** is becoming more and more frequent.
Backup systems are specifically destroyed in 21% of cases.

Attackers are carrying out **increasingly faster attacks** (45% reduction in the time between the intrusion and the triggering of the attack with attacks that succeeded in less than 3 days).

The **duration of crisis is reduced** on average by 2 weeks of interruption and ransoms are paid less and less.
Towards a better preparation?

Benchmark
CERT - 2021

Wavestone, leader in the field of cybersecurity

Wavestone's 600 cybersecurity consultants combine functional, sectoral and technical expertise to cover more than 1,000 missions per year in some twenty 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 & Strategy
- Digital compliance
- Next Generation Cloud & Security
- Penetration testing and security audits
- Incident Response
- Digital identity (for users and customers)

Especially in the field of financial services, industry 4.0, IoT and consumer goods.

Contact our experts

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

Nicolas GAUCHARD
Senior Manager CERT-Wavestone
nicolas.gauchard@wavestone.com
(+33) 667396570