WAVESTONE

Cyber attack in France: what is the situation on the ground?

CERT-Wavestone

September 2018 – August 2019

Tier one clients
leaders in their industry

3,000 professionals
across 8 countries

Among the leading independent
consultancies in Europe,
n°1 in France

Paris | London | New York | Hong Kong | Singapore* | Dubai* | São Paulo*
Luxembourg | Madrid* | Milano* | Brussels | Geneva | Casablanca | Istanbul* | Edinburgh
Lyon | Marseille | Nantes

* Partners

Analysis of cyber attacks affecting large organizations

40

major security incidents

that led to the disruption of business activities or an advanced compromise of the information system

Among the largest French companies and institutions

- ✓ Industry
- ✓ Information Technology
- ✓ Public Sector
- ✓ Finance
- ✓ Retail
- ✓ Services

A study based on the interventions of the Wavestone Security Incident Response Team between September 2018 and August 2019

CERT

CERT-Wavestone

40 cyber experts

Digital Forensics & Incident Response

Crisis management

Malware analysis

Cyber threat analysis

Available 24/7

3x8 organisation during major cyber crisis

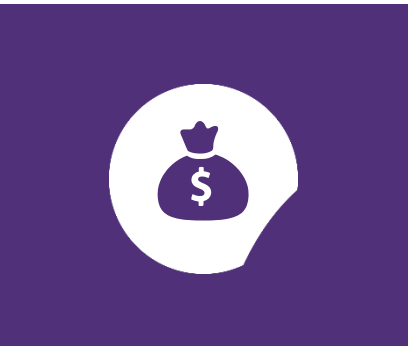
Multi-client

+25 large subscribing organisations

Crisis management expert for several cyber insurances

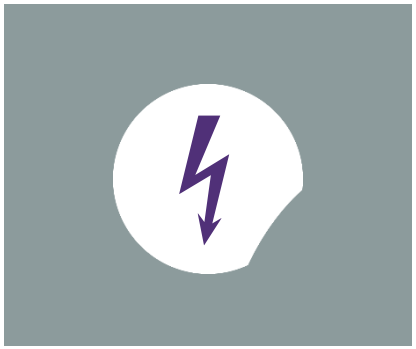
Responses to security incidents benchmark

A willingness to shed light on the state of cyber threat in France and to provide the keys for improved anticipation and reaction



What are the motivations behind cyber attacks?

When and how were they discovered?



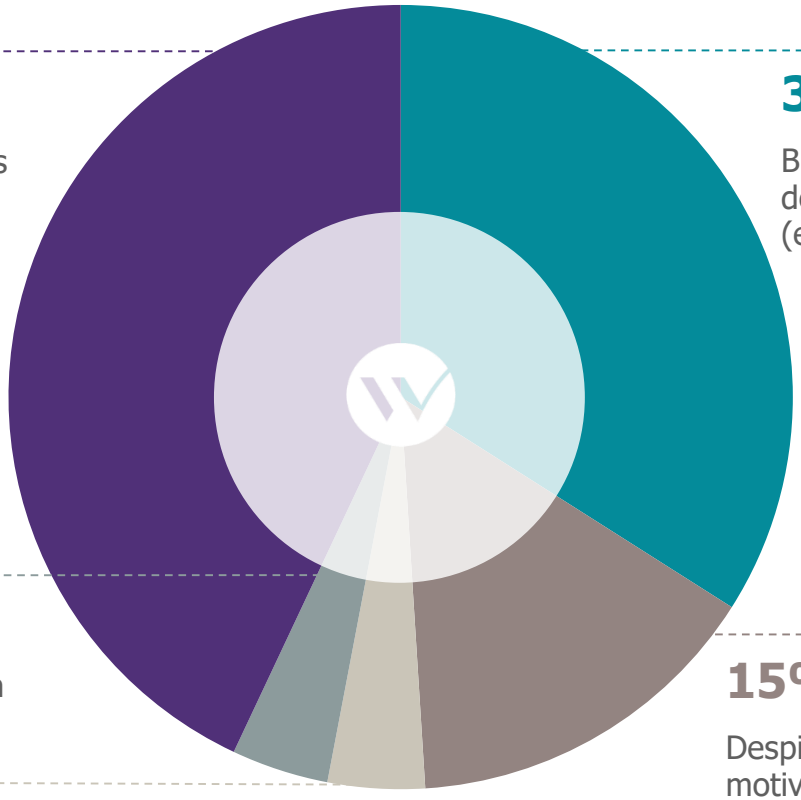
How did they get into the systems?

How to face them and manage the crisis?

How to prepare in advance?

The incentive of financial gain, the main driver for cyber criminals

Distribution of security incidents by attacker motivation



43% financial gain

Including 36% by ransomware attacks and 7% by fraud

34% Data theft

Business data (e.g. customer contact details, bank data...) and technical data (e.g. list of user accounts)

4% Image damage

Website defacement, account theft on social networks

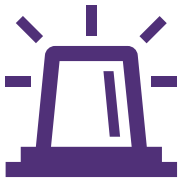
15% Undetermined

Despite the attack, the attacker's motivations could not be identified (attack abandoned, interrupted, systems compromised without further action...)

4% Gains in attack ability

Misappropriating information or resources to conduct an attack on another target

Very heterogeneous detection capabilities among the large companies supported



167 days

Average time elapsed between an intrusion and its detection

But still...

50%

of companies detect the intrusion within two days

35%

of companies only detect the intrusion within 6 to 9 months

6 years

the maximum delay observed between the start of an attack and its detection by one of the companies in the panel....

More than 50% of the attackers do not have advanced technical skills

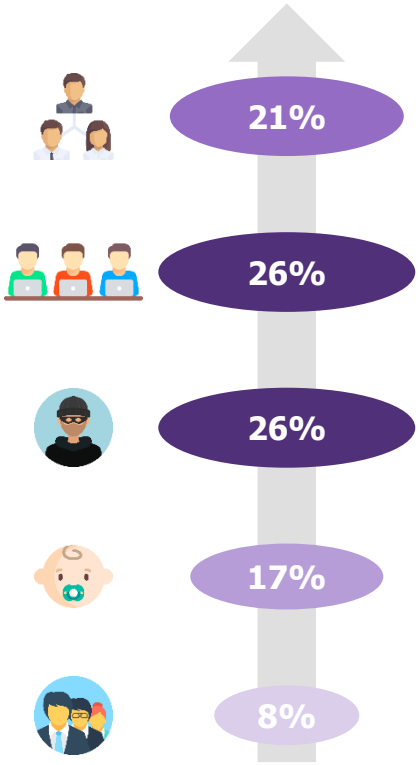
What types of threat?

65% opportunistic threats : often not highly technical; does not target a particular organisation, so if one is more secure than another, attackers will move on to throw themselves at the easiest prey.

30% targeted threats : targets sensitive and precise information in the organisation. The attackers are mandated with a clear objective. They make all the means available to achieve their goals.

5% diffuse threats : corresponds to the usual virus infections or spam; does not target a particular organization and has a limited effect on the IS: denial of service, loss of user data....

Which attacker profiles?



Established organisations
e.g. mafia group developing its own offensive tools to carry out its attacks

Groups of individuals
e.g. team of pirates capable of implementing an offensive methodology using market tools

Cybercriminals
e.g. individual purchasing off-the-shelf piracy services

Script kiddies
e.g. students reusing operating codes and public tools

Insiders
e.g. Malicious collaborators

The same entry gates are regularly used by the attackers

1 in **10** cases

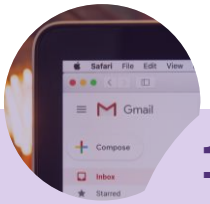
The attacker infiltrated the IS by exploiting an **exposed RDP service**

RDP is a standard mechanism for remote access to computer systems

1 in **3 cases**

The attacker exploited a **vulnerable web application**

100% of web applications are vulnerable according to Wavestone's benchmark audit (wavestone.com)



1 in **10** cases

The attacker infiltrated the SI through **a spear-phishing**

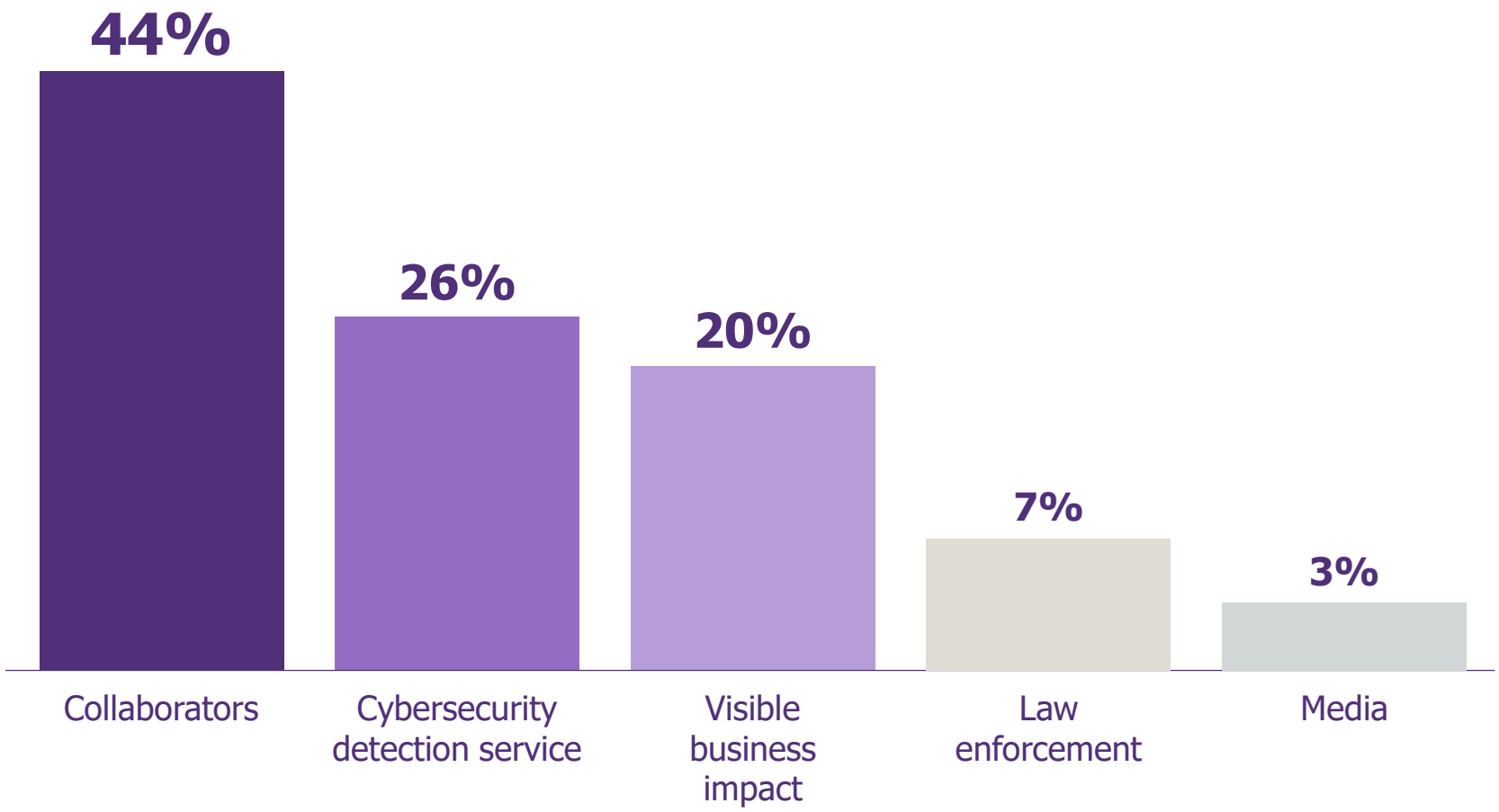
A spear-phishing is a targeted phishing: it targets a specific company or group of users

In 20% of cases, it was not possible to identify the intrusion vector:

- **Insufficient technical traces**
- **Decommissioned or destroyed systems**
- **Lack of local resources**

End users: the cornerstone for attack detection

Breakdown by source of detection of security incidents



Teams to manage the crisis resolution

12
people on average

440
people at most

Of which
25%
are service providers on average

How long does it take to return to a **normal technical situation**?

1 week
For "simple" ransomware (i.e. without propagation)

3,5 weeks
For an attack or ransomworm that has destroyed a significant part of the information system

And at least 6 weeks for a healthy reconstruction, with two key actions:
Reconstruction of the IS's trusted core to switch to a new healthy environment over a weekend
Cleaning and re-importing of business data created during the crisis

A major obstacle at the core of the crisis!

Notorious difficulties in recovering backed up data... due to an unavailability of the backup server (destruction and loss of the backup catalogue) or a loss of integrity of the backups (infection prior to the oldest backup)

The backup server is never backed up....

How to avoid becoming a target?

65%
of attacks are opportunistic

Being above average in cybersecurity allows to strongly limit its attractiveness to cybercriminals

TOP 5 actions to prepare in order to face an attack

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

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

Know how to manage a major crisis (24/7 team, specific means of communication...) **and rebuild in an emergency** (procedures, specific equipment...)

Train through crisis exercises (repeat efforts in different situations to promote the development of reflexes)

Subscribe to cyber-insurance and a contract with a specialized team (surround yourself with experts who can speed up the resolution of the incident)

WAVESTONE

Contact CERT-Wavestone

+33 (0)1.49.03.27.26

cert@wavestone.com
PGP : 1CFEDF1D

Our security incident response and crisis management team available 24/7

https://www.securityinsider-wavestone.com/

wavestone.com
@wavestone_

PARIS

LONDRES

NEW YORK

HONG KONG

SINGAPOUR *

DUBAI *

SAO PAULO *

LUXEMBOURG

MADRID *

MILAN *

BRUXELLES

GENEVE

CASABLANCA

ISTANBUL *

LYON

MARSEILLE

NANTES

* Partenariats

WAVESTONE