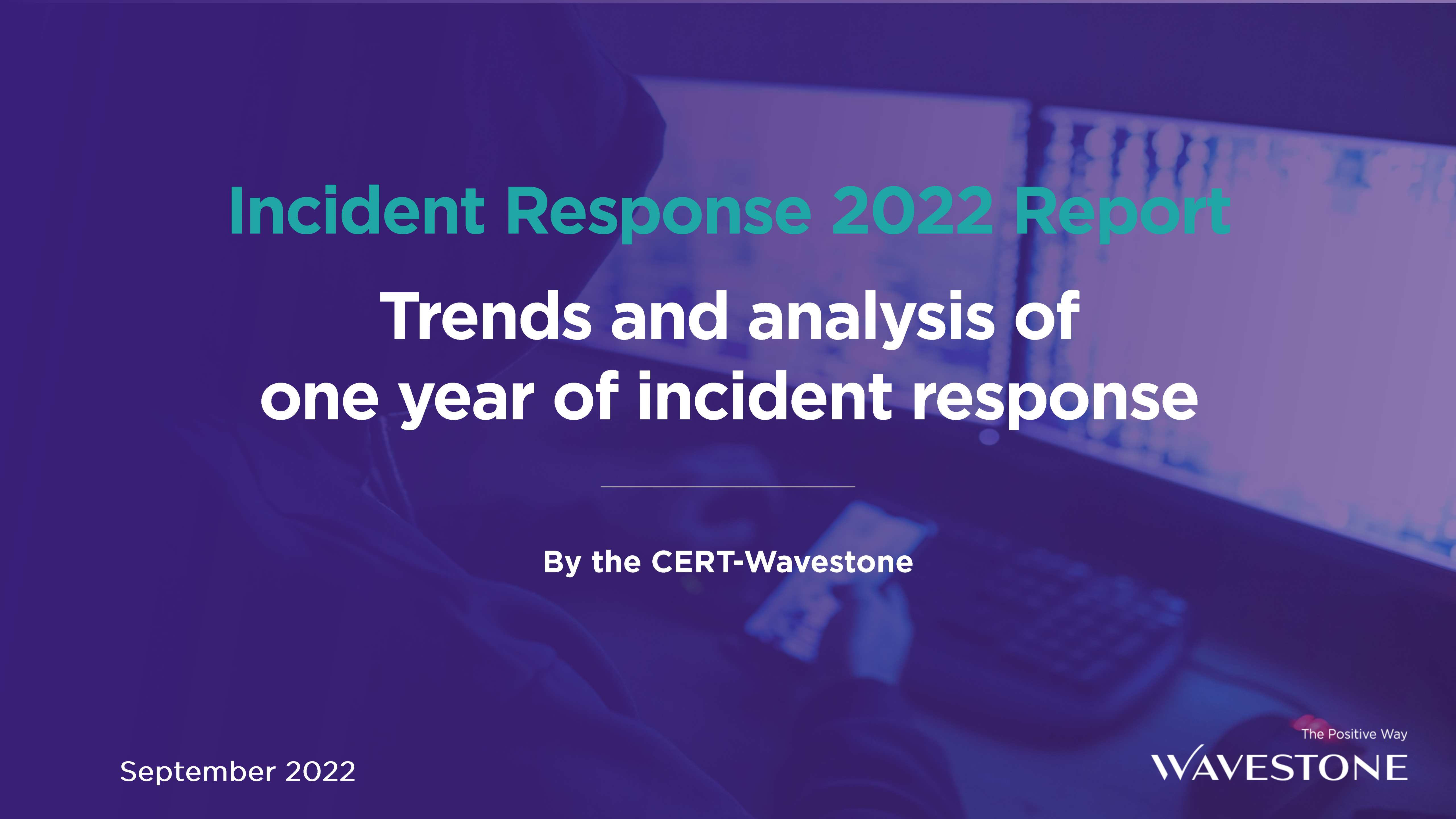


Incident Response 2022 Report

Trends and analysis of one year of incident response

By the CERT-Wavestone

September 2022

The Positive Way

WAVESTONE

Wavestone

We support large enterprises and organizations in their most critical transformations

470 M€

~ 4 000
employees

15 offices
in 9 countries

Business
Technology
Sustainability

Wavestone's CERT-W
40 cyber crisis experts

During cyber incidents...

- / **Forensics investigations**
  System analysis, network analysis, code analysis
- / **Crisis management**
  Steering, anticipation, support to internal and external communication, support to regulatory obligations
- / **Cyber Defense**
- / **Remediation & Reconstruction**
- / **Threat Hunting**

...and before them

- / **Crisis drills**
- / **Cyberattacks simulations**
  Red-team / purple-team
- / **SOC and CERT processes definition, maturity evaluation, trainings**
- / **Cyber Watch**
- / **Evaluation of companies cyber resilience**
- / **Cyber attacks technical analysis**

VISA DE SÉCURITÉ
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION • ANSSI •

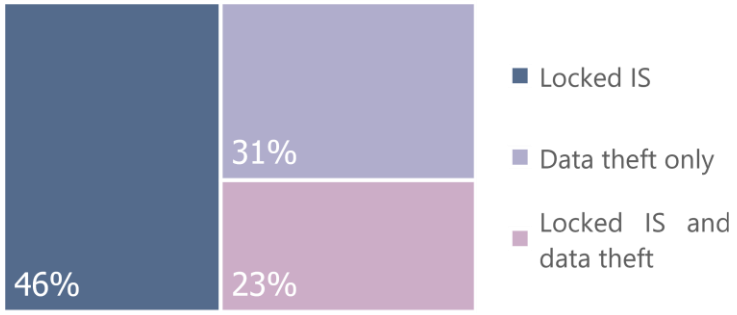
Wavestone is the first company qualified as an "Incident Response Service Provider" (PRIS) by ANSSI.

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

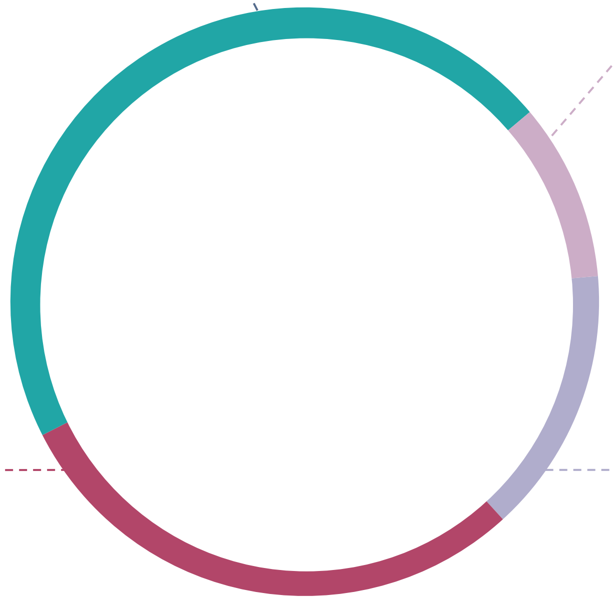
Financial gain remains the main motivation for attackers, hence the predominance of ransomware

Financial gains (51%)

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



75% in 2021



Internal threat & voluntary malevolence (9%)

Not observed in 2021

Internal threat is less visible but remains a real concern that organizations should cover

Preparation for the next cyberattack (32%)

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

10% in 2021

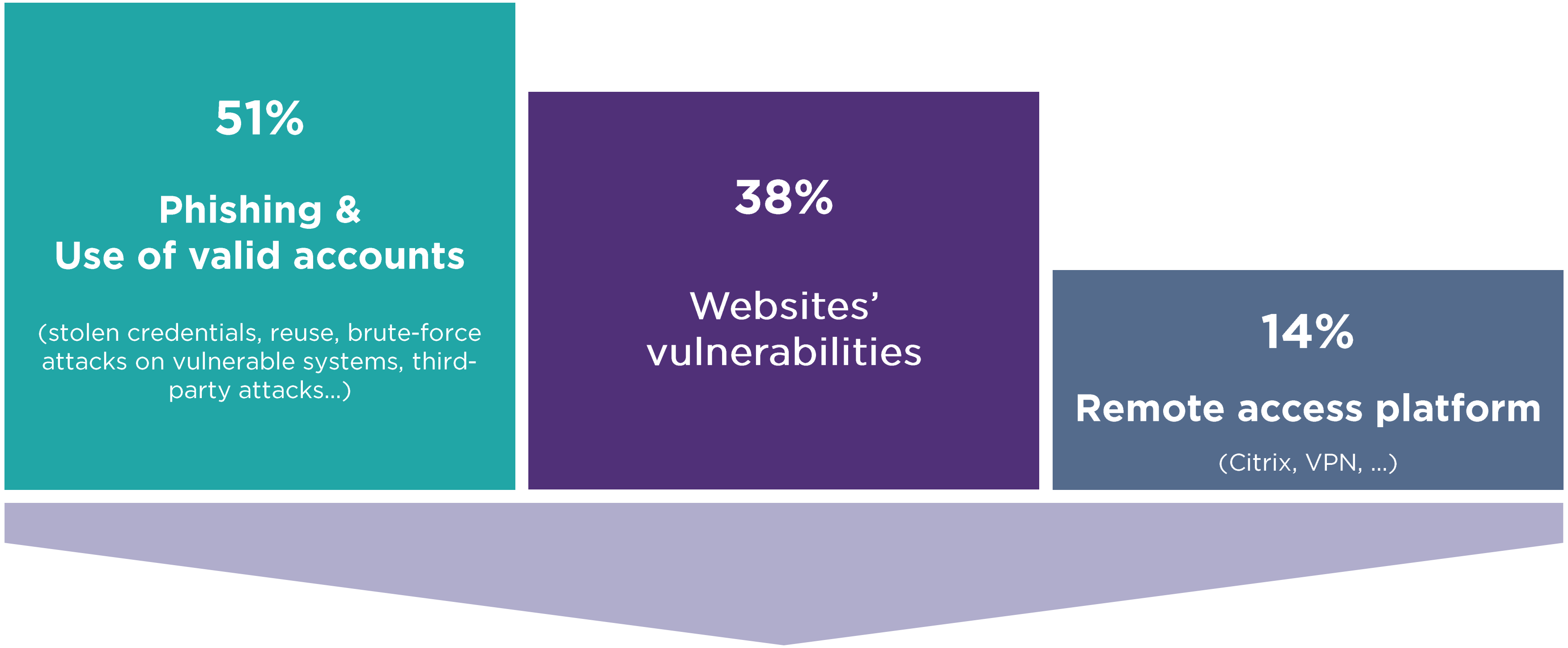
Undetermined (16%)

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

15% in 2021

Sabotage and espionage are two other important motivations for attackers, but these cases are mostly handled by ANSSI.

Use of stolen accounts is still the main way for attackers to get into their victim's systems



51%

Phishing &
Use of valid accounts

(stolen credentials, reuse, brute-force attacks on vulnerable systems, third-party attacks…)

38%

Websites' vulnerabilities

14%

Remote access platform

(Citrix, VPN, …)

On-premise Active Directory infrastructures are still a key target for attackers and were involved in **8 out of the 9** cyber crisis tackled by CERT-W during the 2021-22 period.

Of the 9 large-scale crisis that were handled by the CERT-W in 2021/22:

→ **2 out of 9** were directly caused by a **third-party compromise**

→ **4 out of 9** impacted adversely the **organization's partners**

Attacks remain largely opportunistic in nature

All sectors and company size are targeted, but large companies are less likely to fall victim than small companies and public sector organizations…

76%

of the incidents handled by the CERT-W are **deemed opportunistic**, i.e., they are attacks that **do not target a particular organization**.

116

ransomware attacks were recorded for the **first three quarters of 2022**. A total of 237 attacks were recorded in 2021, and 129 in 2020.*

Only 3

large companies are known to gave fallen **victim of cyber attacks in 2022** (11 in 2021, 16 in 2020).*

23

attacks were recorded for the **first three quarters of 2022, targeting public sector organizations (health, governance, education)** A total of 47 such attacks were recorded in 2021, and 40 in 2020.*

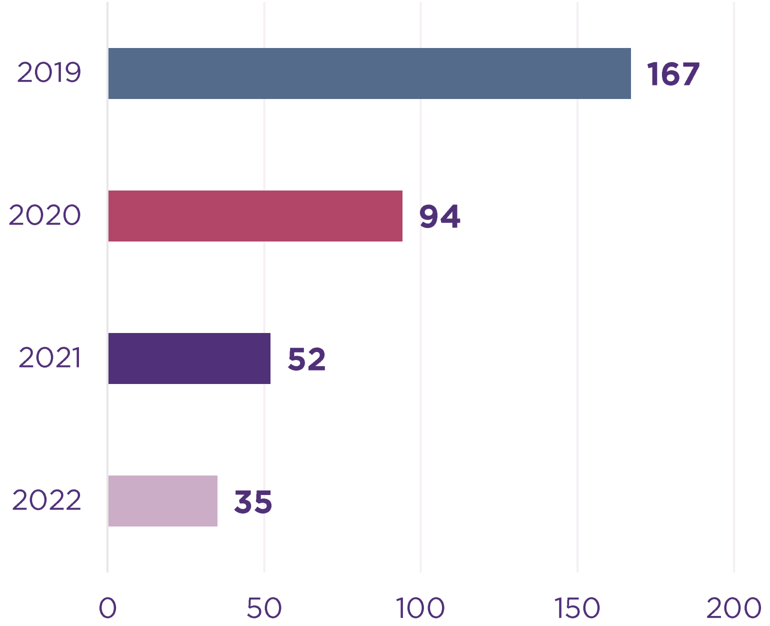
*Data taken from publications by Valéry Rieß-Marchive (LeMagIT)

This is explained also by large companies investing in cybersecurity

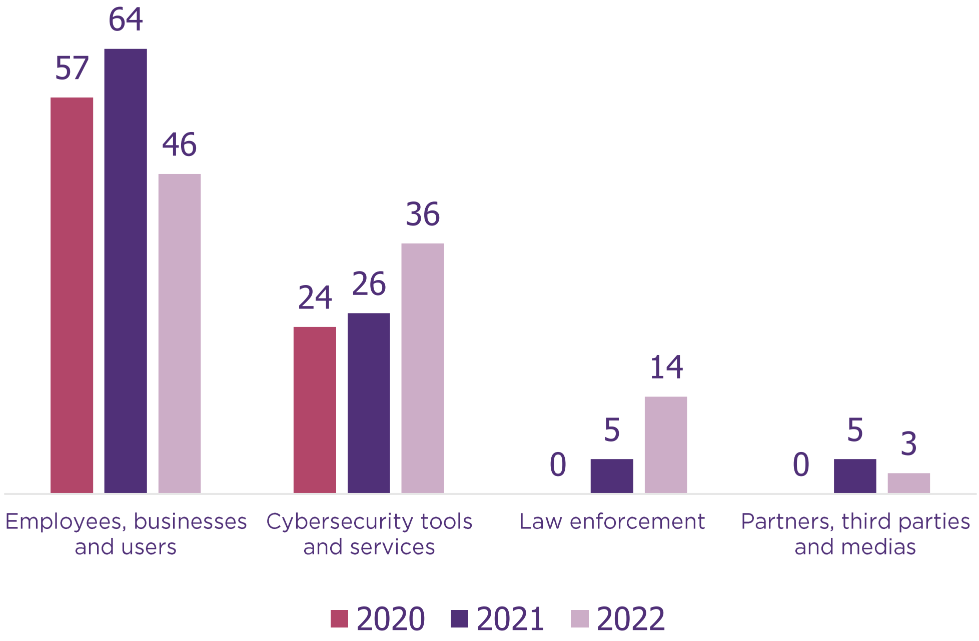
In practical terms, this means shorter detection and reaction times as well as increasing efficiency of cybersecurity tooling…

Delay between initial intrusion and detection

35 days



Distribution by source of detection of security incidents

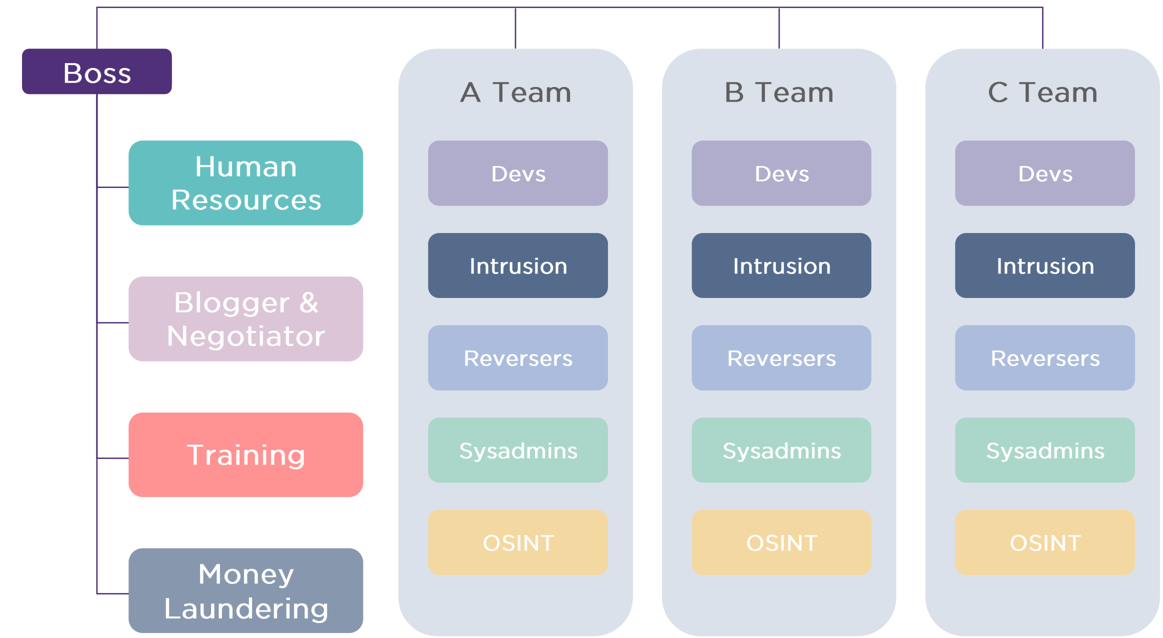


Benchmark CERT - 2022

What's next: attackers are getting more organized

The Conti documents leaked in early 2022 tell us a lot about how criminal organizations are getting more and more structured…

Conti internal organization chart



Read our full study on the Conti leaks on Wavestone's blog Risk Insight

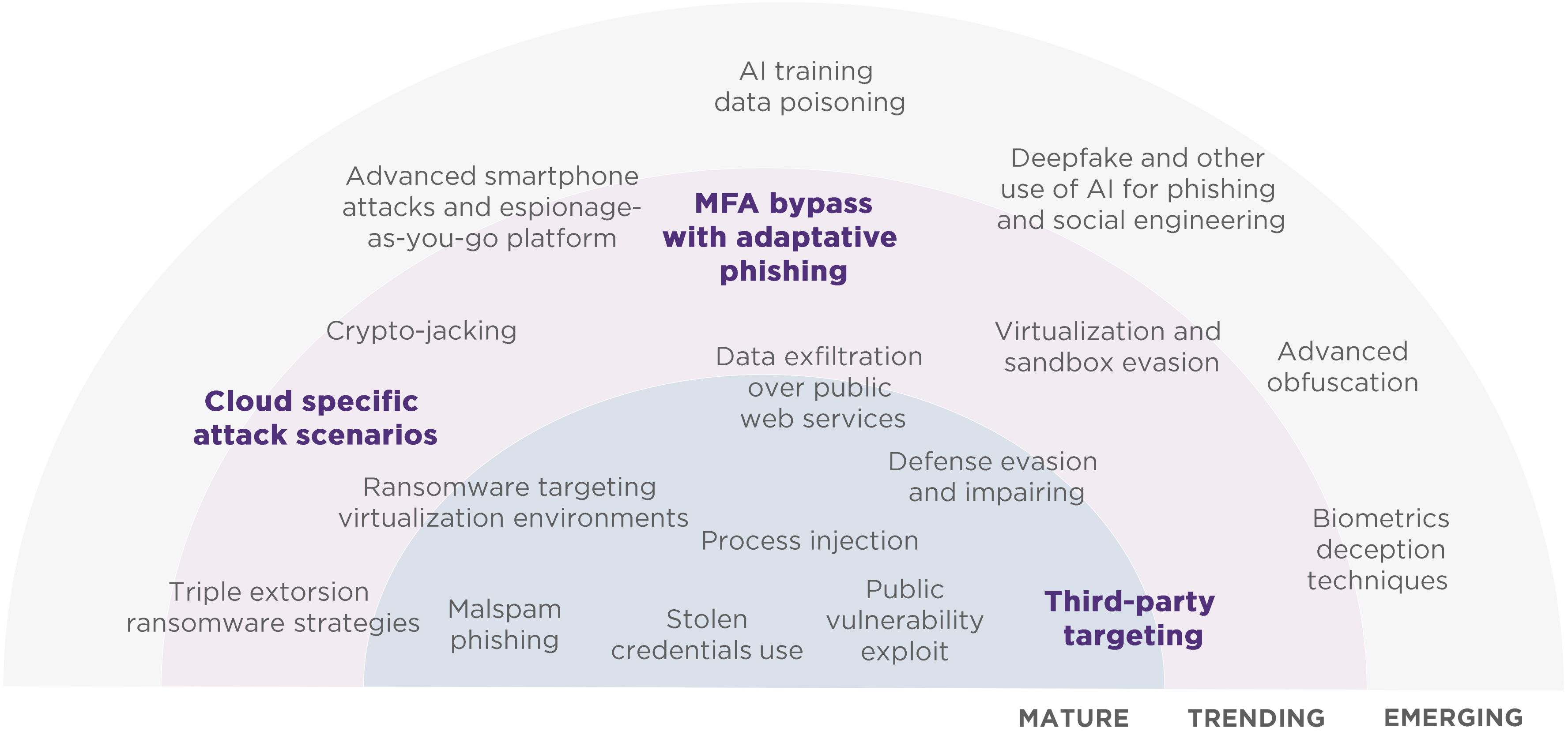
With structures looking more and more like a **corporate organization** (with departments like sourcing, HR or training) counting close to **100 employees**, the criminal groups now have time to:

→ **concentrate expertise** on specific activities

→ **train their employees to be more efficient**

© WAVESTONE

Attacker’s skills are on the rise… What to look at?



AI training data poisoning

Advanced smartphone attacks and espionage-as-you-go platform

MFA bypass with adaptative phishing

Deepfake and other use of AI for phishing and social engineering

Crypto-jacking

Virtualization and sandbox evasion

Advanced obfuscation

Data exfiltration over public web services

Cloud specific attack scenarios

Defense evasion and impairing

Ransomware targeting virtualization environments

Process injection

Biometrics deception techniques

Triple extorsion ransomware strategies

Malspam phishing

Stolen credentials use

Public vulnerability exploit

Third-party targeting

MATURE

TRENDING

EMERGING

Cloud attack scenarios

Exploiting badly configured cloud environments to access company resources or data, gain admin capabilities and get a foothold into company systems.

Led to leak of Tesco customer information and crypto mining malware activity on Tesla's cloud assets

MFA Bypass

Using advanced phishing techniques and social engineering technics to replay MFA credentials submitted by victims or sending of thousand of authentication request to users to force acceptance of MFA requests.

Led to Uber and Twilio incidents in 2022

Third party

Use of third-party accounts or information systems to penetrate the target.

Led to 4 of the 9 major crisis we managed in 2022

Companies need to keep investing to defend against new attacks

What you can do to prepare...

Strengthen your cloud security policies across the whole organization.
Build **inventories** of SaaS/IaaS/PaaS and **identify dependencies** stemming from third party cloud services.

Build and **maintain a third-party lifecycle management process**, with periodic recertification of accesses, active audits and shared resilience plans and exercises.

Perform **"red team" operations** with an emphasis on social engineering and advanced phishing techniques to **prepare key users** to react properly in suspicious situations.

...without forgetting about the basics!

A resilient, robust and tested backup and restore strategy

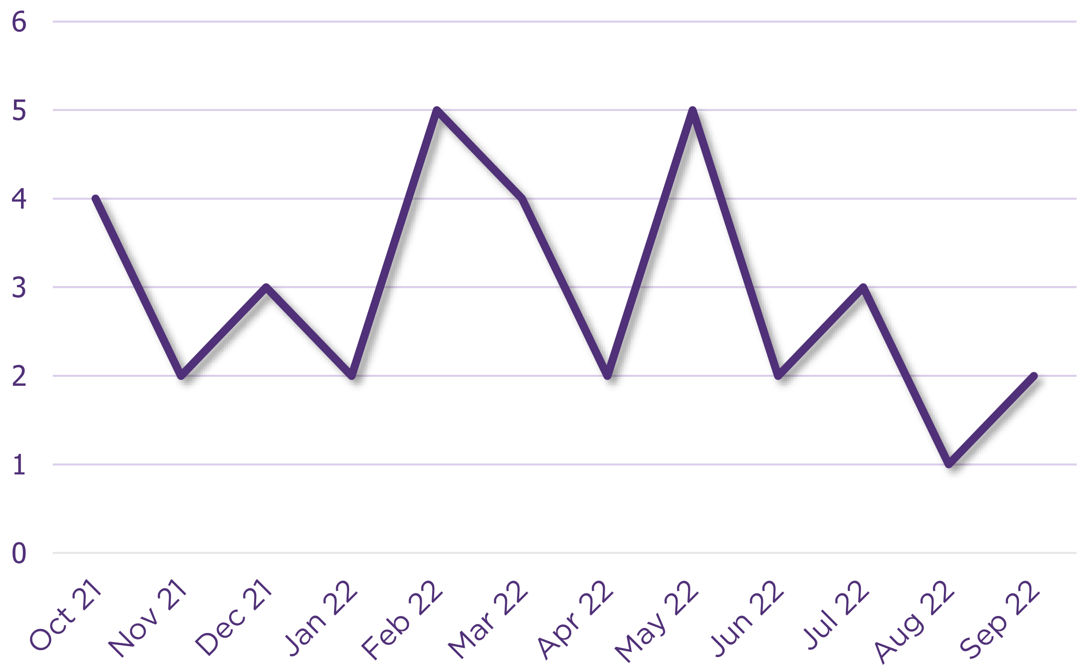
A crisis organization, with dedicated tooling and highly-trained people

An efficient detection toolset with a process to monitor its efficiency

A cyber-insurance and specialized support from experts

Summary of the cyberattacks handled by the CERT-W

Number of major cyber incidents impacting our clients



This study was based on the cyber incidents and crisis handled by the CERT-W team between the months of October 2021 and September 2022 (included).

35 major cybersecurity incidents

in **large companies or public organizations**, were handled by the CERT-W this year.

For each one of them, **forensics investigations** were required and **direct impacts** on the information system were attested.

Of these, there were **9 cyber-crisis** where the advanced compromise of the information system required a **dedicated crisis organization.**

In a nutshell...

Financial gain draws better-organized cybercriminals to a more vulnerable mid-market

Financial gains remains the first motivation for attackers. Intrusion channels remain the same as previous years, with the notable rise of third-parties attacks.

The threat is **still largely opportunistic**. Large companies are now prepared to face it with better detection and reaction capabilities. **Mid-market and public sector are now the main victims** of attacks.

Criminal organizations are evolving, with **structures now resembling those of the corporate world**, allowing them to benefit from synergies and recruit/train resources more efficiently.

Companies, large or small, will need to **keep investing, training and pushing awareness** to be able to defend against the future threats coming from attackers

Wavestone,
leader in the field of cybersecurity

Wavestone's 700 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

Robin OLIVIER
Manager CERT-Wavestone
robin.olivier@wavestone.com
(+33) 7 63 97 32 50