Rapport du CERT-W 2022

Tendances et analyses d'un an de réponses à incidents

Par le CERT-Wavestone

Septembre 2022

The Positive Way
WAVESTONE

Wavestone

Nous accompagnons les grandes entreprises et les organisations dans leurs transformations les plus critiques

470 M€

~ 4 000
employés

15 bureaux
dans 9 pays

Business
Technologie
Environnement

Wavestone CERT-W
40 experts des crises cyber

Durant les incidents cyber...

- **Investigations techniques**
  Analyse des systèmes, des réseaux et des codes
- **Gestion de crise**
  Pilotage, anticipation, soutien à la communication interne et externe, soutien aux obligations règlementaires
- **Stratégies de défense**
- **Remédiation et reconstruction**
- **Identification des menaces**

...et en amont

- **Exercices de crise**
- **Simulation de cyber attaques**
  Red-team / purple-team
- **Définition des processus SOC et CERT, évaluation de la maturité, entraînement**
- **Veille cyber**
- **Evaluation de la cyber résilience des entreprises**
- **Analyses techniques des cyber attaques**

Wavestone est la première entreprise qualifiée « Prestataire de Réponse à Incident de Sécurité” (PRIS) by ANSSI.

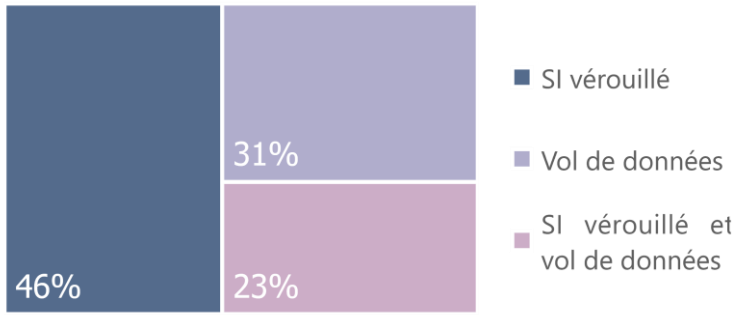
Qualification N°1443 | Validité de 3 ans à partir de 29/06/2020

© WAVESTONE

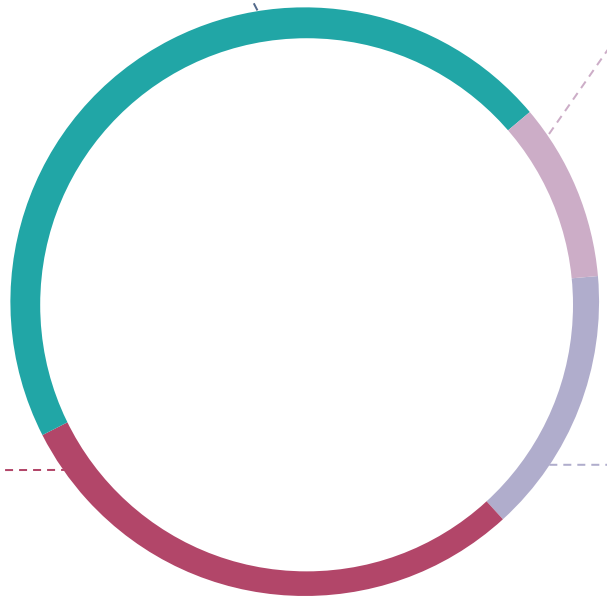
Les gains financiers restent la première motivation des attaquants, et les ransomwares dominent

Gains financiers (51%)

Des gains financiers peuvent être recherchés par le chantage au blocage du SI et/ou à la non-divulgation, ou par la revente des données volées.



75% en 2021



Menace interne et malveillance volontaire (9%)

Aucun cas observés en 2021. La menace interne est moins visible mais reste une préoccupation réelle que les organisations doivent couvrir.

Préparation de la prochaine cyberattaque (32%)

Détournement d'informations ou de ressources pour mener une attaque sur une autre cible (spam/phishing, DDoS, chaîne d'approvisionnement...)

10% en 2021

Indéterminé (16%)

Malgré la compromission, les motivations de l'attaquant n'ont pas pu être identifiées (attaque abandonnée, interrompue, compromission des systèmes sans actions...)

15% en 2021

Le sabotage et l'espionnage sont deux autres motivations importantes pour les attaquants: ces cas sont le plus souvent gérés par l'ANSSI.

© WAVESTONE

L'utilisation de comptes volés est toujours la porte d'entrée principale des attaquants

Les infrastructures Active Directory sont toujours des cibles clés pour les attaquants et ont été impliquées dans **8 crises cyber sur 9** gérées par le CERT-W durant la période 2021-22.

Sur la base de 9 crises d'ampleur gérées par le CERT-W en 2021-22 :

→ **2 sur 9**

ont été directement causées par la **compromission d'un tiers**

→ **4 sur 9**

ont eu un impact violent **sur l'organisation de leurs partenaires**

© WAVESTONE

Les attaques restent de nature opportuniste

Tous les secteurs et les entreprises de toutes tailles sont ciblés, cependant les grandes entreprises **sont moins susceptibles d'en être victimes** contrairement aux petites entreprises et aux organisations du secteur public…

76%

des incidents gérés par le CERT-W **sont réputés opportunistes** : ce sont des attaques qui **ne ciblent pas un type d'organisation en particulier**

116

attaques ransomwares ont été enregistrées **pour les 3 premiers trimestres de 2022.** Au total, 237 attaques ont été enregistrées en 2021 et 129 en 2020.*

3

grandes entreprises sont connues pour avoir été victimes **de cyber attaques en 2022** (11 en 2021, 16 en 2020).*

23

attaques ont été enregistrées pour les 3 premiers trimestres de 2022, **ciblant les organisations du secteur public (santé, gouvernement, éducation)**. Un total de 47 attaques de ce type a été enregistré en 2021 et 40 en 2020.*

**Données provenant des publications de Valéry Rieß-Marchive (LeMagIT)*

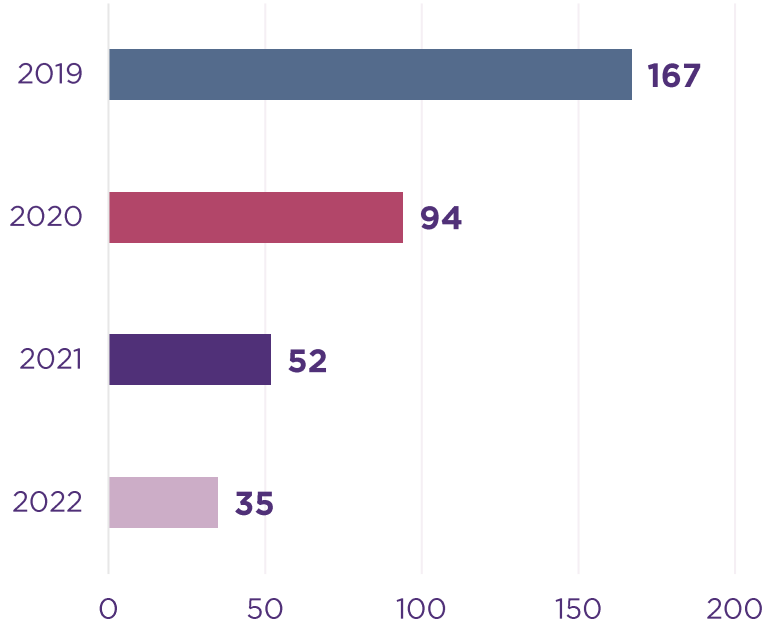
© WAVESTONE

Cela s'explique par l'investissement des grandes entreprises en cybersécurité

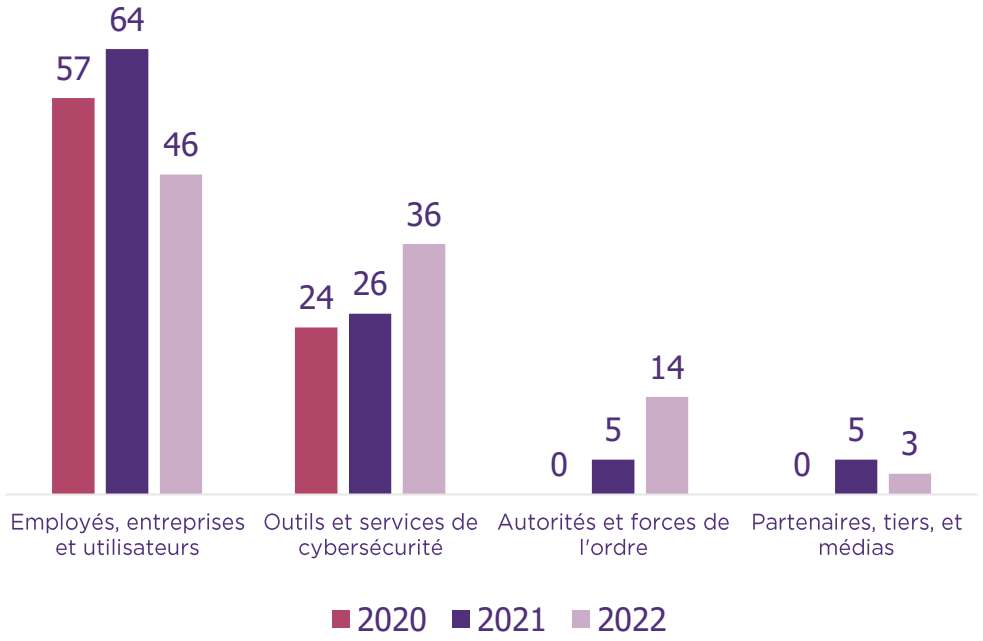
Concrètement, cela signifie des temps de détection et de réaction plus courts, ainsi qu'une efficacité accrue des outils de cybersécurité…

Délai entre l'intrusion initiale et la détection

35 jours



Distribution par source de détection des incidents de sécurité

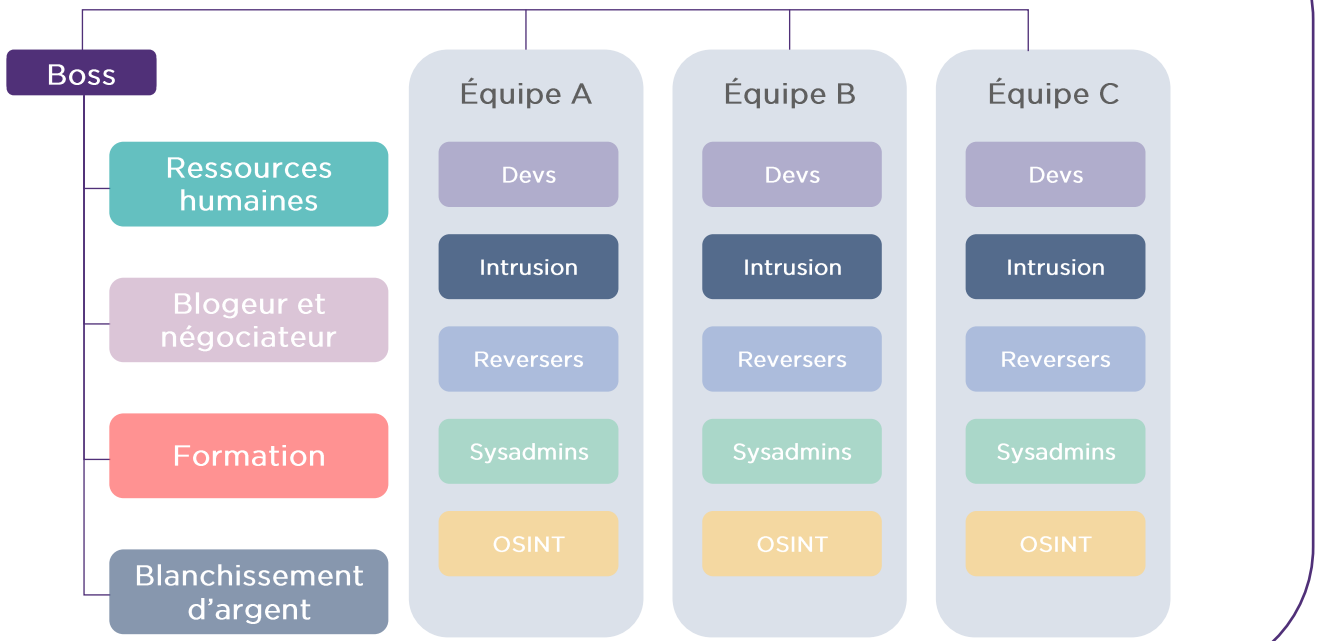


Benchmark CERT - 2022

Et demain? Les attaquants vont continuer à s'organiser

Les documents du groupe Conti, divulgués au début de l'année 2022, nous apprennent beaucoup sur la façon dont les organisations criminelles se structurent de plus en plus...

Organigramme de l'organisation interne de Conti



Lisez notre étude complète sur les fuites de Conti sur le blog de Wavestone Risk Insight

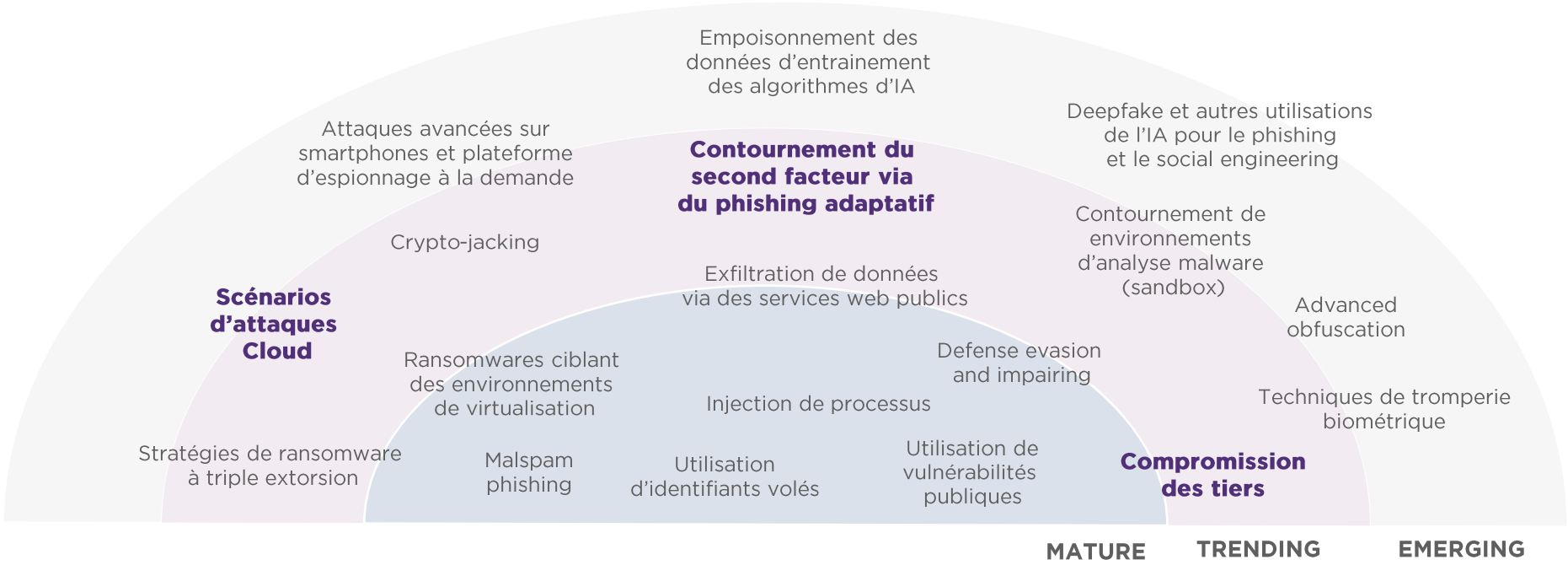
Avec des structures ressemblant de plus en plus à **une organisation d'entreprise** (avec des départements comme l'approvisionnement, les RH ou la formation) comptant près de **100 employés**, les groupes criminels ont désormais le temps de :

→ **concentrer leur expertise** sur des activités spécifiques

→ **former leurs employés** pour qu'ils soient plus efficaces

© WAVESTONE

Les compétences des attaquants sont croissantes… que faut-il regarder ?



Scénarios d'attaques Cloud

Exploitation d'environnements cloud mal configurés pour accéder aux ressources ou aux données de l'entreprise et obtenir des capacités d'administration sur les systèmes de l'entreprise.

A conduit aux fuites d'informations sur des clients de Tesco et à l'exploitation de serveurs pour le minage de crypto-monnaie sur le Cloud de Tesco

Contournement de l'authentification multi-facteurs

Utilisation de techniques de phishing avancées et de techniques d'ingénierie sociale pour rejouer les informations d'authentification soumises par les victimes ou envoi de milliers de demandes d'authentification second-facteur aux utilisateurs pour les forcer à accepter les demandes.

A conduit aux incidents d'Uber et Twilio en 2022

Tierce partie

Utilisation de comptes ou de systèmes d'information de tiers compromis au préalable pour compromettre le système d'information cible.

A conduit à 4 des 9 crises majeures que nous avons gérées en 2022

© WAVESTONE

Les entreprises doivent continuer à investir pour se défendre contre de nouvelles attaques

Ce que vous pouvez faire pour vous préparer...

Renforcez vos politiques de sécurité Cloud dans l'ensemble de l'organisation. **Dressez des inventaires** des SaaS/IaaS/PaaS et **identifiez les dépendances** découlant des services cloud utilisés au sein de votre organisation.

Élaborer et **maintenir un processus de gestion du cycle de vie des tiers**, avec certifications périodiques des accès, des audits actifs et des plans de résilience et exercices de crise partagés.

Effectuer des **opérations "Red team"** en mettant l'accent sur le social engineering et les techniques avancées de phishing pour préparer les utilisateurs clés à réagir correctement dans les situations suspectes.

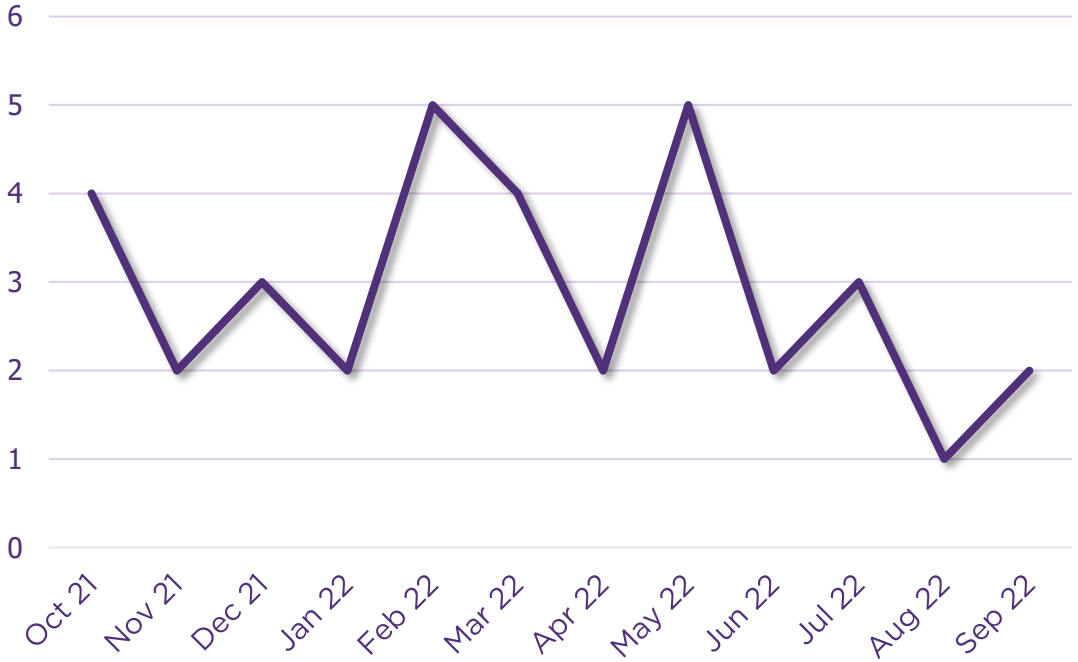
...sans oublier les basiques !

- Une stratégie de sauvegarde et de restauration résiliente, solide et testée
- Une organisation de crise, avec un outillage dédié et un personnel hautement qualifié
- Un ensemble d'outils de détection efficace avec un processus pour contrôler son efficacité
- Une cyber-assurance et un soutien spécialisé de la part d'experts

© WAVESTONE

Résumé des cyberattaques gérées par le CERT-W

Nombre d'incidents cyber majeurs ayant impacté nos clients



CERT

Cette étude s'est basée sur les incidents cyber et les crises traités par l'équipe du CERT-W entre les mois d'octobre 2021 et septembre 2022 (inclus).

35 incidents de sécurité majeurs

dans de **grandes entreprises ou des organismes publics**, ont été traitées par le CERT-W cette année.

Pour chacune d'entre elles, des **investigations forensiques** ont été nécessaires et **des impacts directs** sur le système d'information ont été constatés.

Parmi celles-ci, on compte **9 crises cyber** où la compromission avancée du système d'information a nécessité **une organisation de crise dédiée**.

© WAVESTONE

En synthèse…

Le gain financier attire les cyber criminels mieux organisés vers des organisations intermédiaires plus vulnérables

Les gains financiers restent la première motivation des attaquants.
Les canaux d'intrusion restent les mêmes que les années précédentes, avec l'augmentation notable des attaques par des tiers.

La menace est **encore largement opportuniste**. Les grandes entreprises sont désormais préparées à y faire face grâce à de meilleures capacités de détection et de réaction.
Le marché intermédiaire et le secteur public sont désormais les principales victimes des attaques.

Les organisations criminelles évoluent, leurs structures ressemblant désormais à celles du monde de l'entreprise, ce qui leur permet de bénéficier de synergies et de recruter/former des ressources plus efficacement**.**

Les entreprises, grandes ou petites, devront **continuer à investir, à se former et à sensibiliser leurs collaborateurs** pour être en mesure de se défendre contre les futures menaces des attaquants.

© WAVESTONE

Wavestone,
leader dans le domaine de la cybersécurité

Les 700 consultants en cybersécurité de Wavestone combinent des expertises fonctionnelles, sectorielles et techniques pour couvrir plus de 1 000 missions par an dans une vingtaine de pays (dont la France, le Royaume-Uni, les États-Unis, Hong Kong, la Suisse, la Belgique, le Luxembourg et le Maroc).

Une expertise éprouvée de la stratégie à la mise en œuvre opérationnelle :

- Gestion des risques et stratégie
- Conformité numérique
- Cloud nouvelle génération et sécurité
- Tests de pénétration et audits de sécurité
- Réponse aux incidents
- Identité numérique (pour les utilisateurs et les clients).

Notamment dans le domaine des services financiers, de l'industrie 4.0, de l'IoT et des biens de consommation.

Contacter nos experts

Gérôme BILLOIS
Associé Cybersecurité
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