# Rapport du CERT-W 2023

# Tendances et analyses d'un an de réponses à incidents

Par le CERT-Wavestone

Septembre 2023

# Wavestone

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

**530 M€**

**~ 4 500**
employés


**15 bureaux**
dans 9 pays

**Business**
**Technologie**
**Environnement**

Qui sommes-nous ?

# 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**
- **Renfort CSIRT**
- **Simulation de cyber-attaques**
  *Red-team / purple-team*
- **Définition des processus SOC/CSIRT, évaluation de maturité, entraînement**
- **Veille cyber**
- **Evaluation de la cyber résilience**
- **Analyses techniques des attaques**

Wavestone fait partie des quatre entreprises qualifiées **"Prestataire de Réponse aux Incidents de Sécurité"** (PRIS) par l'ANSSI.



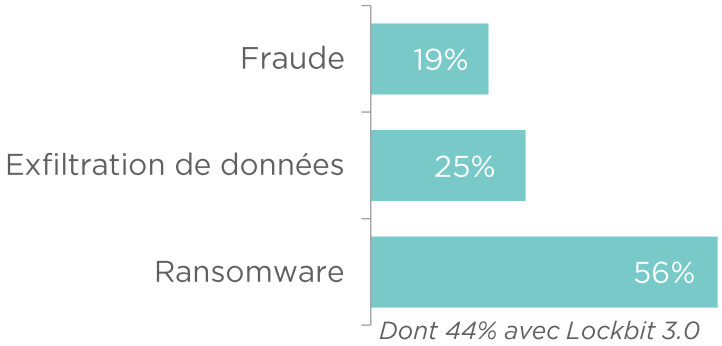
Quelles sont les motivations des attaquants ?

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

## Gains financiers (46%)

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. Des cas de fraude sont réapparus cette année.

*51% en 2022*

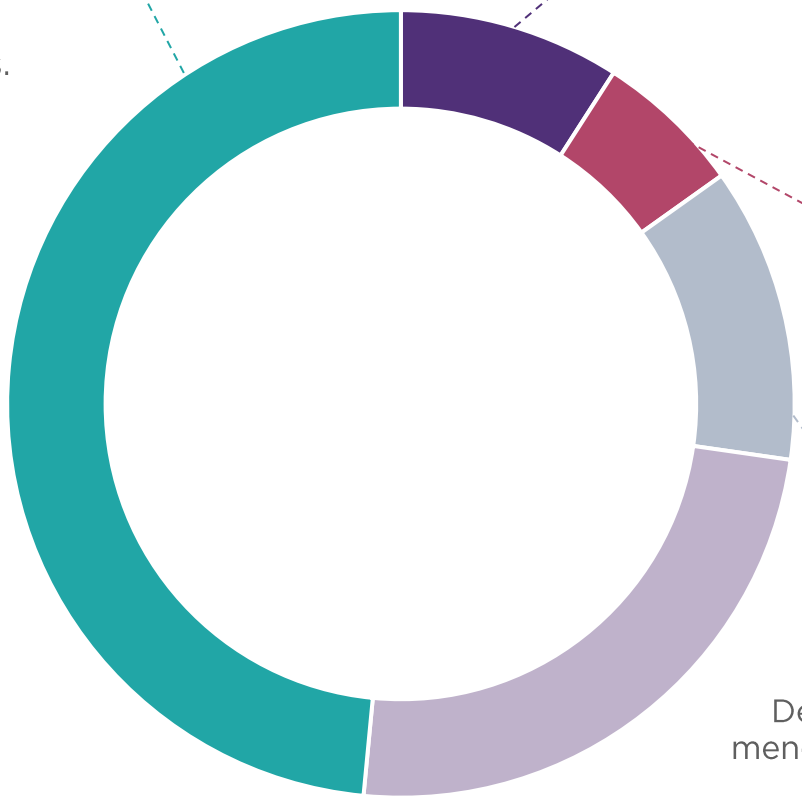



*Dont 44% avec Lockbit 3.0*

## Indéterminé (29%)

Malgré la compromission, les motivations de l'attaquant n'ont pas pu être identifiées (attaque stoppée avant l'impact, compromission des systèmes sans actions, impacts non significatifs...)

*16% en 2022*



## Malveillance (6%)

Avec une majorité de cas de malveillance interne visant à supprimer des données, des acteurs externes agissent également via des attaques de défacement.

*9% en 2022*

## Espionnage (9%)

Non identifié sur nos accompagnements par le passé, les attaques répondant à cette motivation sont une conséquence du contexte géopolitique tendu.

*0% en 2022*

## Préparation de la prochaine cyber-attaque (11%)

Détournement d'informations ou de ressources pour mener une attaque sur une autre cible (spam/phishing, compromission O365, intrusion physique...)

*32% en 2022*



Quels vecteurs d'attaque utilisent-ils ?

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

**42%**

**Phishing & utilisation de comptes volés préalablement**

(vol d'identifiants valides, réutilisation, attaques par force brute sur des systèmes vulnérables, attaques de tiers...)

**23%**

**Vulnérabilités des sites web**

**17%**

**Via les systèmes d'accès à distance**

(Citrix, VPN, ...)

***Tendance 2023***

**Compromission des comptes Office 365**

*devenus la solution de bureautique standard dans les entreprises*

**facilitée par l'absence d'authentification multi-facteurs (MFA)**

**Les infrastructures Active Directory** sont toujours des cibles clés pour les attaquants et ont été impliquées dans **1 crise cyber sur 2** gérée par le CERT-W durant la période 2022-23.



Quelles sont les cibles des attaquants ?

# Les attaques restent de nature opportuniste

Si tous les secteurs et toutes les tailles d'entreprises sont ciblés, quatre tendances se confirment :

## Des structures touchées de plus en plus petites

Les grandes entreprises ont amélioré leurs **capacités de détection** et réponse sur les dernières années et sont moins touchées par les attaques

En réponse, les cybercriminels s'orientent vers des **cibles plus simples** et moins matures en cybersécurité

## Des données de plus en plus visées

**77%** des cas de **ransomwares** observés **combinent chiffrement et exfiltration de données**, et la note de rançon fait quasi-systématiquement mention du vol de données

La menace de publication des données volées est devenue **le moyen de pression le plus efficace** des attaquants

## Des attaques de plus en plus rapides et multiples

**Le temps d'exécution** d'une attaque par **ransomware diminue fortement**, passant de plusieurs semaines à quelques jours

**Des attaques impliquant de multiples ransomwares** font ainsi leur apparition, visant la même victime à quelques jours d'intervalle

## Des infrastructures utilisées comme effet de levier

Les environnements ou **plateformes de virtualisation** de type ESXi sont devenus l'une des cibles préférées des attaquants

Ces plateformes permettent de toucher plusieurs centaines voire milliers de serveurs virtuels **en une attaque**



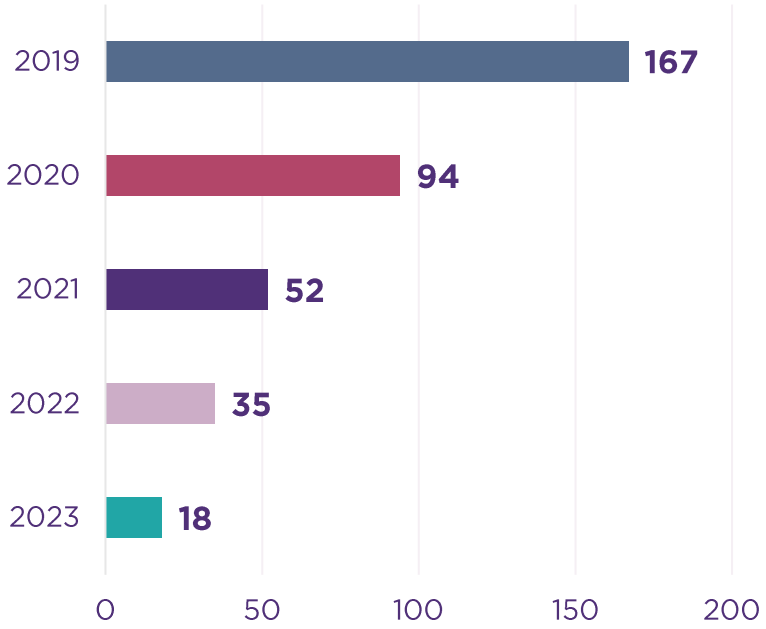
# Un investissement en cybersécurité des grandes organisations qui porte ses fruits

Temps de détection plus courts, efficacité accrue des outils de cybersécurité, capacités de réaction en hausse…

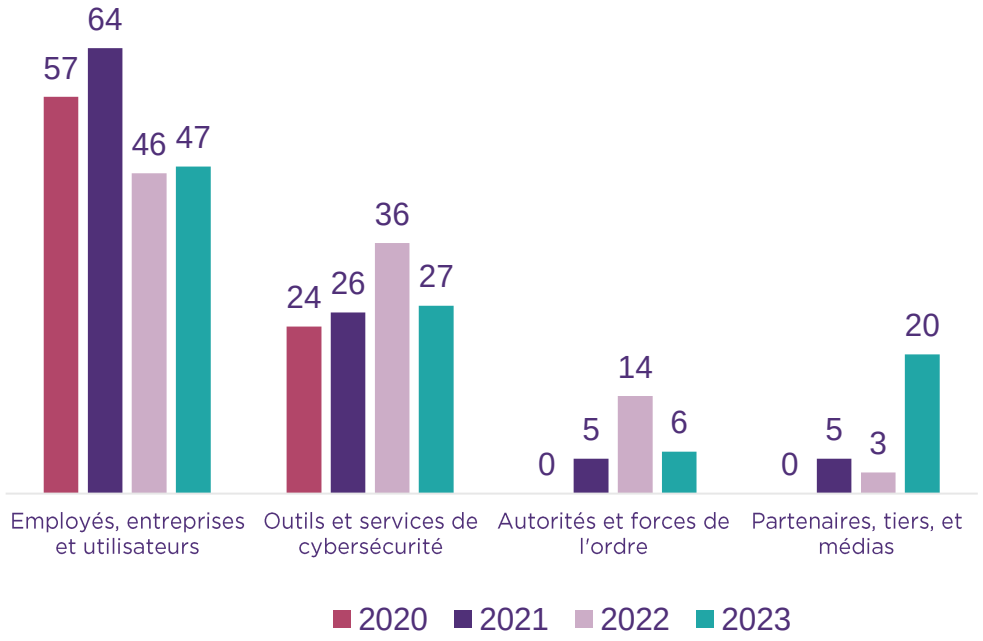
## Délai entre l'intrusion initiale et la détection

**18 jours**

Contre **71 jours** en moyenne pour les petites et moyennes entreprises




## Distribution par source de détection des incidents de sécurité





# Nouvelles situations d'urgence : le découplage de SI face à une menace provenant d'un tiers

**Isoler un périmètre géographique**
En cas de contexte géopolitique tendu

**Isoler une entité ou une fonction métier**
En cas de compromission ou de crainte par rapport à un SI spécifique

## Déclenchement de la gestion de crise pour assurer un premier niveau de découplage en quelques jours

**Protéger le cœur d'activité *(Minimum Viable Company)***

Pour assurer la résilience des processus métier vitaux des applications critiques

**Cloisonner les réseaux**

Pour n'autoriser que les communications strictement nécessaires

**Augmenter le niveau de surveillance**

Pour être en mesure d'identifier et de bloquer toute tentative d'action malveillante

**Investiguer de manière proactive**

Pour rechercher des traces de compromissions antérieures ou postérieures à la prise de contrôle du périmètre hostile

**Quelle stratégie adopter ?**

**Carve-out rapide :** Gagner du temps pour se protéger, mais s'exposer à des **risques d'espionnage**

***VS***

**Coupure du SI :** Se protéger sans délais, mais s'exposer à des **risques de représailles** (cyber-attaque, action juridique, etc.)



Quelle menace majeure anticiper pour les années à venir ?

# L'Intelligence Artificielle générative,

## Des nouvelles capacités pour les cybercriminels...

**DÉTOURNEMENT DE SOLUTIONS**

*Rédaction de documents frauduleux, conception de logiciels malveillants, injection de messages, etc.*

**NOUVEAUX OUTILS**

*Automatisation des attaques, variation de malware existant, etc.*

**UTILISATION DE DEEPFAKE**

*Personnalisation du phishing, vol d'identité par imitation vocale ou détournement d'image, etc.*

## ...mais également de nouvelles cibles, vulnérables à des attaques innovantes

**ChatBots de vente en ligne**

**Systèmes anti-fraude**

**Systèmes de détection**

**Décision automatisée**

### Attaques par empoisonnement

/ Des jeux de données
/ Lors de l'entraînement et du réentraînement de l'IA

### Attaques par manipulation

/ Évasion
/ Reprogrammation de modèle
/ Déni de service

### Attaques par déduction

/ Déduction de l'appartenance
/ Extraction de modèles
/ Inversion de modèles

Benchmark CERT - 2023

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

## Ce que vous pouvez faire pour vous préparer aux futures menaces…

**Identifier et être prêt à protéger le cœur d'activité *(Minimum Viable Company)* :** cartographier les **processus métiers vitaux** au sein des applications critiques, déployer des mesures de protection adaptées, être en mesure de les isoler et de les reconstruire rapidement.

**Augmenter le niveau d'attention** vis-à-vis des nouveaux risques liés à l'usage de l'IA, **évaluer la sécurité des systèmes d'IA interne,** sensibiliser les collaborateurs et **revoir les processus métiers** qui pourraient être impactés (détection de fraude, etc.)

### Jeux Olympiques - Paris 2024

**Anticiper toutes attaques cyber** pouvant viser l'évènement, ses partenaires, ou la population de manière indirecte (ex : fraudes)

**S'assurer de la disponibilité des équipes et des partenaires cyber** en prenant en compte que l'évènement se tiendra au cœur de la période estivale

## …sans oublier les bonnes pratiques !

**Définir une stratégie de protection contre les fuites de données** *(Data Loss Prevention)* et **adopter une attitude proactive** face aux menaces d'exfiltrations de données métiers et d'infrastructures (ex : base Active Directory)

Déployer une **authentification multi-facteurs** (MFA) sur l'ensemble des environnements exposés sur internet, et notamment sur les **environnements O365**

**Protéger les infrastructures supportant le cœur d'activité** (cloisonnement, suivi des vulnérabilités et des correctifs de sécurité, gestion des droits, etc.), **y compris en cas de virtualisation et dans le cloud**



# La motivation financière reste prédominante, menaçant les organisations de plus petite taille

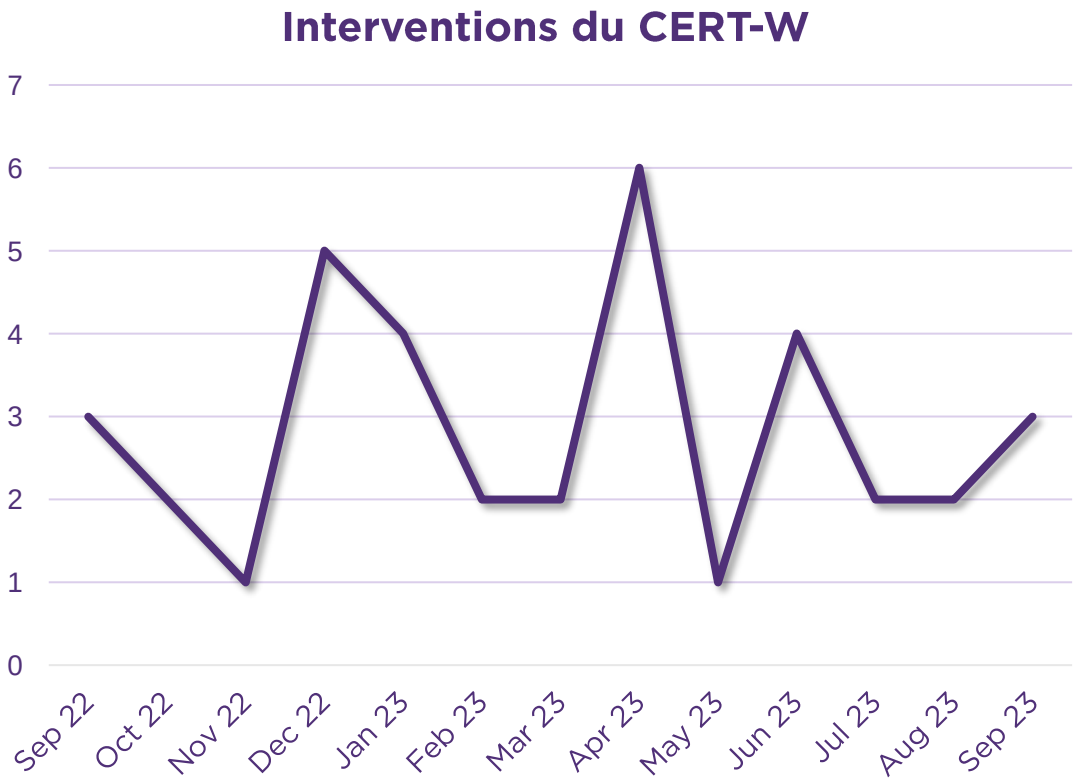
**Les gains financiers restent la première motivation des attaquants**.
Les canaux d'intrusion restent les mêmes, avec principalement l'utilisation de comptes valides, souvent non sécurisés.

La menace est **encore largement opportuniste**. Comme les grandes entreprises y sont mieux préparées, la menace se **décale vers le marché des petites et moyennes entreprises**.

**Les organisations criminelles s'organisent et s'industrialisent toujours plus**. Ces structures se radicalisent dans le contexte géopolitique actuel, répondant à une motivation de déstabilisation.

Les investissements paient pour les grandes entreprises, qui doivent **continuer à investir, se former et sensibiliser leurs collaborateurs** pour être en mesure de se défendre contre les futures menaces.

# Résumé des cyber-attaques gérées par le CERT-W




CERT

Cette étude s'est basée sur les incidents cyber et les crises traités par l'équipe du CERT-W entre les mois de septembre 2022 et de septembre 2023 (inclus).

## 37 incidents de sécurité majeurs

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

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

Parmi ceux-ci, on compte **16 crises cyber** où la compromission avancée du système d'information a nécessité **une organisation de crise dédiée**.



# Wavestone,
## leader dans le domaine de la cybersécurité

900 consultants en cybersécurité qui 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 d'intrusions et audits de sécurité
- Réponse aux incidents
- Identité numérique (pour les utilisateurs et les clients)

Une expérience dans de nombreux domaines, notamment dans les services financiers, l'industrie 4.0, l'IoT et les biens de consommation

## Contacter nos experts

**Gérôme BILLOIS**
Associé Cybersecurité
gerome.billois@wavestone.com
(+33) 6 10 99 00 60
@gbillois

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