Rapport 2024

Tendances et analyses d'un an de réponses à incidents

Par le

CERT WAVESTONE

WAVESTONE

Wavestone : une offre de conseil à forte valeur ajoutée

360° une proposition de valeur holistique

17 pays une force de frappe mondiale

+5 500 employés

943,8 M€ de chiffre d'affaires pro forma

Indépendants pragmatiques et orientés résultats

Le CERT-Wavestone : 40 experts spécialistes des crises cyber

Durant les incidents…

- Investigations et analyse forensics
  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
- Formation et renfort de CSIRT
- Simulation de cyber-attaques
  RedTeam / Purple-team
- Evolution des SOC et CSIRT
  Evaluation de maturité, entraînement, plan d'actions
- Campagne de phishing
- Evaluation de la cyber résilience
- Evaluation de l'empreinte Internet
- Cyber Threat Intelligence

Wavestone a été la première entreprise à recevoir et à renouveler sa certification **"Prestataire de Réponse aux Incidents de Sécurité" (PRIS)** par l'ANSSI sur tous les périmètres :

- Recherche d'Indicateurs de Compromission [REC]
- Investigation numérique sur Périmètre Restreint [IPR]
- Investigation numérique sur Large Périmètre [ILP]

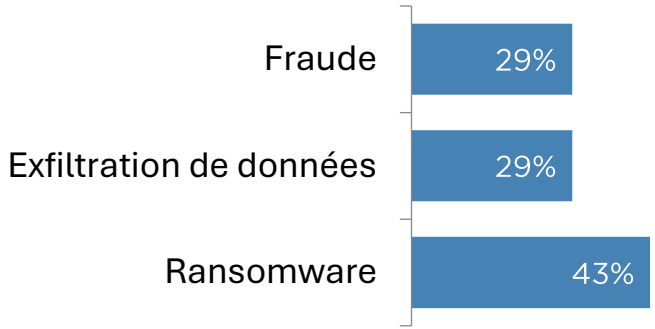
Ce rapport constitue l'analyse des 20 incidents majeurs traités par le CERT-Wavestone entre août 2023 et septembre 2024

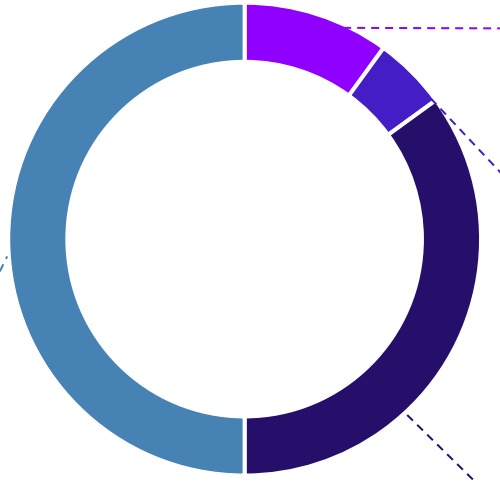
Les gains financiers restent la première motivation des attaquants, et les ransomwares dominent

Gains financiers (50%)

Principalement au travers du blocage du système d'information, de la menace de divulgation d'informations volées ou de fraudes persistantes.

46% en 2023, 51% en 2022





Espionnage (10%)

De plus en plus fréquentes chaque année, ces attaques sont alimentées par un contexte géopolitique tendu.

8% en 2023, 0% en 2022

Malveillance interne (5%)

Avec pour objectif le vol de données internes dans la majorité des cas, notamment lors des départs.

6% en 2023, 29% en 2022

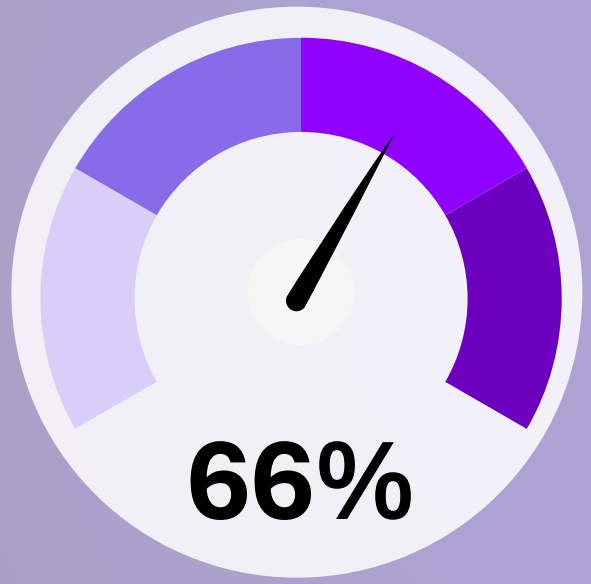
Indéterminées (35%)

Les motivations de l'attaquant restent inconnues (absence d'impact, attaque interrompue, etc.)

29% en 2023, 16% en 2022

Des grandes entreprises touchées notamment au travers de leurs filiales ou leurs partenaires

Les progrès en cybersécurité des grandes entreprises les protègent face aux menaces les plus courantes, mais leurs filiales les moins matures restent vulnérables.



des attaques ciblant les grandes entreprises ont visé des filiales.

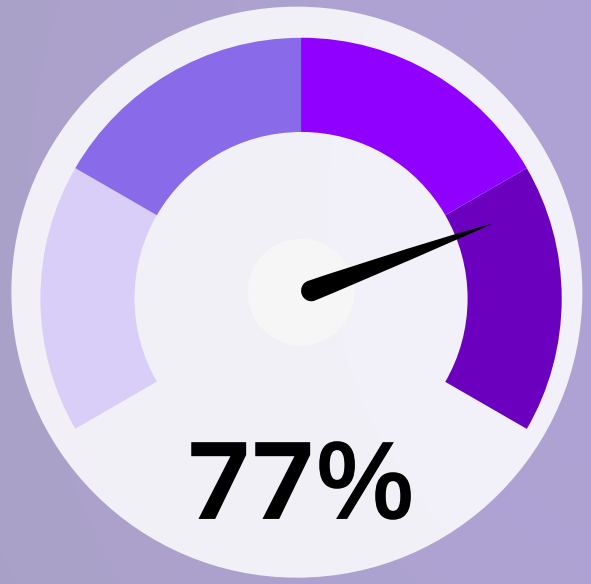
Retour terrain : une attaque par ransomware sur une filiale

Une filiale d'un groupe du **secteur banque - assurance** a été attaquée via une vulnérabilité critique sur un **composant exposé sur Internet** et non maintenu à jour.

L'attaquant a ensuite profité de règles de filtrages permissives pour **se propager sur le système d'information**, **extraire des données** et lancer **le ransomware.**

La compromission des données métiers : un objectif privilégié des attaquants

Que ce soit pour de l'espionnage ou pour inciter le paiement d'une rançon, le vol de données reste l'un des principaux impacts des cyber-attaques.



77%

des attaques ont comporté un vol de données avéré.

Retour terrain : un espionnage de données métier sur 2 ans

Un attaquant a maintenu un accès persistant **pendant 2 ans** sur le système d'information d'une entreprise **du secteur industriel**.

Cela lui a notamment permis d'exfiltrer des emails à intervalle régulier.

Sa présence n'a été révélée que lorsqu'une campagne de phishing a été menée depuis l'une des adresses compromises.

La vigilance et la réactivité des entreprises mises à l'épreuve par les attaquants

Les attaques étant de plus en plus rapides, les capacités de détection et de réaction automatisées des SOC et CERT sont clés pour contrer les cyber-attaques.

3 jours

entre l'intrusion et l'impact de l'attaque (plus court délai constaté).

Retour terrain : une attaque éclair de type ransomware

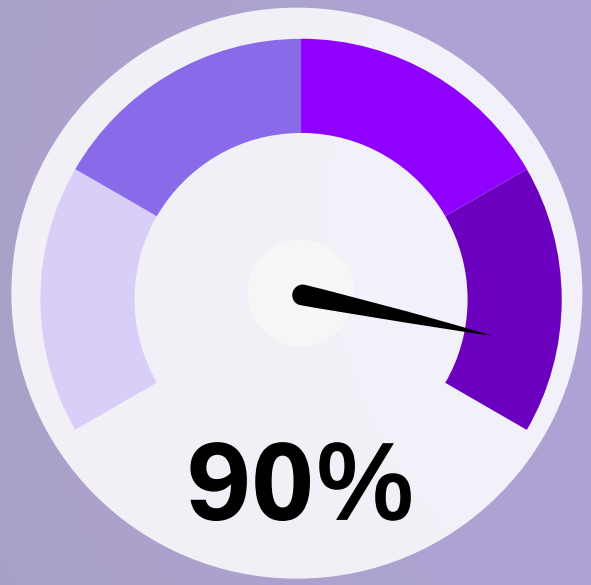
Un attaquant a obtenu par brute force l'accès à un compte local de la passerelle **VPN**.

En moins de 2 heures, il a élevé ses privilèges et compromis le domaine Active Directory au travers de comptes de services.

Pendant les 2 jours suivants, **l'attaquant a exfiltré massivement des données**, puis a lancé son attaque par ransomware le week-end.

Les sauvegardes : cible de choix des attaquants pour bloquer la reconstruction

L'effacement des sauvegardes est un objectif de plus en plus courant pour les attaquants afin de positionner le paiement de la rançon comme seule option pour les victimes.



des attaques ransomwares ont ciblées directement ou indirectement les sauvegardes.

Retour terrain : des sauvegardes compromises pour empêcher la reconstruction du SI

Dans le secteur de la santé, un attaquant est devenu **administrateur de l'Active Directory.**

Il a ensuite **désactivé la réalisation de nouvelles sauvegardes, et désactivé le système d'alerte** supervisant leur réalisation.

Enfin, l'attaquant a **attendu une dizaine de jours** pour déclencher son attaque par ransomware, s'assurant ainsi que la victime ne dispose pas de sauvegarde récente pour reconstruire.

Les vulnérabilités des sites web exposés, le premier canal d'entrée vers le SI

20%

42% en 2023

Phishing et utilisation de comptes volés préalablement

Permettant une élévation de privilège en passant par l'ADCS, la CI/CD ou les outils d'hypervision.

40%

23% en 2023

Exploitation de vulnérabilités des sites web exposés

Permettant une exécution de code à distance, l'accès non autorisé à des bases de données ou la prise de contrôle des serveurs.

20%

17% en 2023

Intrusion via les systèmes d'accès à distance (Citrix, VPN, etc.)

Permettant un accès direct aux systèmes critiques de l'entreprise

Verbatims des équipes RedTeam Wavestone

« 100% des missions RedTeam ont trouvé des mots de passe stockés dans des espaces de partage. »

« Notre équipe RedTeam est capable de déployer un outil d'exploitation automatisé quelques jours seulement après la publication d'une CVE. »

L’Intelligence Artificielle, une nouvelle arme à disposition des cybercriminels

Génération de script malveillant

L’IA permet de générer des scripts malveillants qui **facilitent la recherche de vulnérabilités** et **la réalisation d’attaques** par des acteurs de faible niveau d’expertise.

Grâce à une IA, Google a récemment découvert une faille inconnue dans le code source de SQLite.

Des chercheurs d’HP suspectent l’usage de l’IA pour développer le code malveillant permettant de lancer le téléchargement du malware AsyncRAT.

Phishing

L'IA améliore les possibilités de phishing en **automatisant et en perfectionnant** ces attaques pour les rendre encore plus réalistes

Selon Proofpoint, les tentatives de phishing ont augmenté de ~30% au Japon, en Corée et aux Emirats Arabe Unis suite à l’introduction de ChatGPT.*

Deepfake

L'IA facilite l’usurpation d’identité (et en particulier les arnaques au président) **à travers de faux audios ou vidéos**

A Hong Kong , un collaborateur s’est fait piégé par un Deepfake lors d’une visio conférence, ce qui a coûté 26 millions d’euros à l’entreprise

*2024 State of The Phish Report

L'Intelligence Artificielle, une opportunité pour des attaques encore méconnues

Empoisonnement

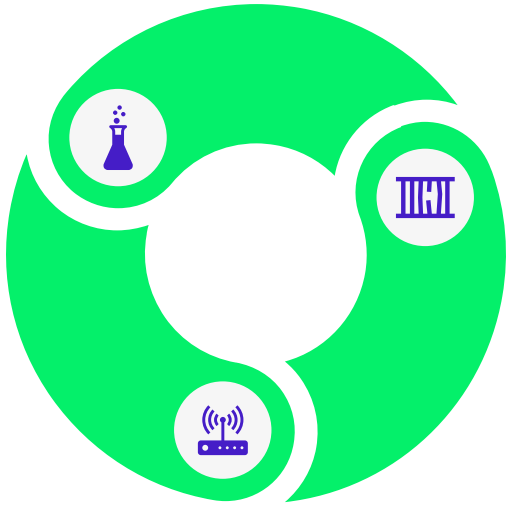
L'attaquant manipule des données d'entraînement pour **nuire à l'intégrité du modèle d'IA.**

Plus de 100 modèles empoisonnés sont disponibles sur la plateforme Hugging Face[1]

Oracle

En interagissant avec le modèle d'IA, l'attaquant tente **d'extraire des informations** sur les données d'entraînement ou sur le modèle en lui-même.

Des dizaines de projets visant à transformer Copilot en "Copirate" sont disponibles sur Github[2]



Evasion

Les attaques par évasion impliquent la modification minutieuse des données d'entrée **pour conduire le modèle à des décisions erronées.**

Plusieurs dizaines d'outils de prompt injection pour ce type d'attaque sont disponibles sur GitHub

Les environnements de développement des outils d'IA, à l'instar des outils de data, sont aussi exposés aux attaques standards car les bonnes pratiques de sécurité ne sont pas toujours appliquées.

[1]*Plateforme de mise à disposition de modèles d'IA* [2]*Source : "Microsoft Copilot: From Prompt Injection to Exfiltration of Personal Information"*

Les entreprises doivent investir dans les mesures ayant le plus d'impact dans la protection contre les attaques

Gestion des identités

- Maîtriser de bout en bout la gestion des comptes à privilèges (PAM)
- Sécuriser les référentiels d'identités au même titre que les assets les plus critiques

Supervision

- Assurer la couverture complète du parc (EDR)
- Mettre en place une gouvernance assurant le bon niveau de réactivité
- Maîtriser ses vulnérabilités sur l'ensemble du SI

Sauvegarde

- Sécuriser et surveiller les systèmes de sauvegarde
- Isoler les sauvegardes de l'Active Directory
- Réaliser des copies hors ligne ou immuables des sauvegardes

… sans oublier les périmètres les moins maîtrisés

Filiales

- Auditer et contrôler le niveau de maturité cyber des filiales
- Maîtriser l'ensemble des interconnexions avec les filiales
- Établir un processus « Red Button » pour isoler les filiales

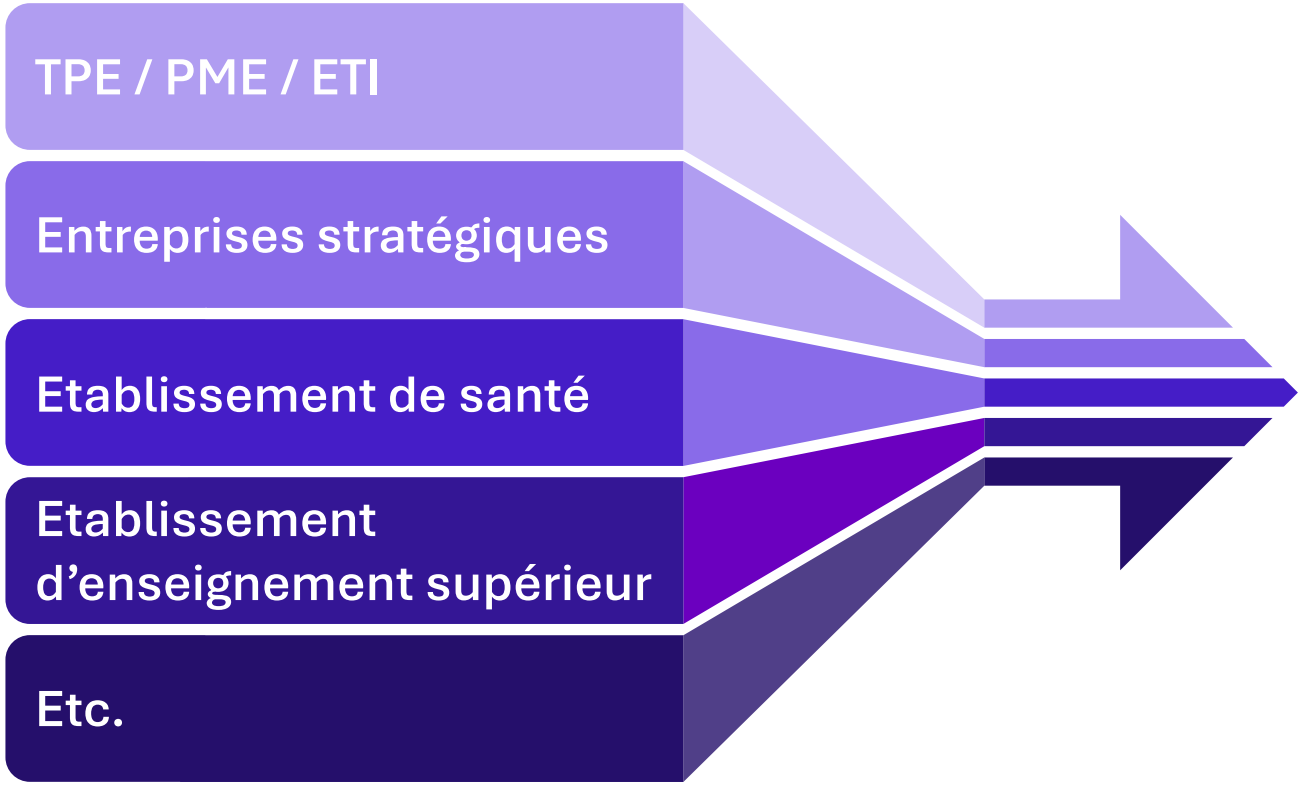
Cloud

- Clarifier les modèles de gestion du cloud
- Appliquer systématiquement le principe du moindre privilège
- Contrôler automatiquement l'application du durcissement

IA

- Sécuriser les environnements de développements de l'IA
- Mener des exercices de crise avec des scénarios IA
- Se doter d'une équipe d'investigation sur l'IA

Des attaques gérées par le CERT-Wavestone sur l'ensemble des secteurs et des tailles d'entreprise



20 incidents de sécurité majeurs

Plus de 10 secteurs différents ont été accompagnés par le CERT-Wavestone cette année, les principaux correspondant aux cibles majeures identifiés par l'ANSSI.

Que ce soit en France ou à l'international, **à chaque fois des investigations forensiques ont été nécessaires**.

Wavestone,

Leader dans le domaine de la cybersécurité

1 000 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 et gestion de crise
- 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 (0)6 10 99 00 60
𝕏 @gbillois

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