Rapport 2025

Analyse d’un an de réponses à incidents et évolutions des menaces

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

+6 000 employés

943,7 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

- Renfort de CSIRT
- Exercices de crise
- Simulation de cyber-attaques
  RedTeam / Purple-team / Cyber Range
- 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-LPM)** par l'ANSSI sur tous les périmètres :

- Recherche d'Indicateurs de Compromission [REC]
- Investigation numérique [INV]
- Analyse de code malveillants [CODE]
- Pilotage et coordination des investigations [PCI]

Ce rapport constitue l'analyse des 21 incidents majeurs traités par le CERT-Wavestone entre août 2024 et septembre 2025 sur de multiples secteurs d'activités (entreprise stratégiques, établissement de santé, enseignement supérieur, etc.).

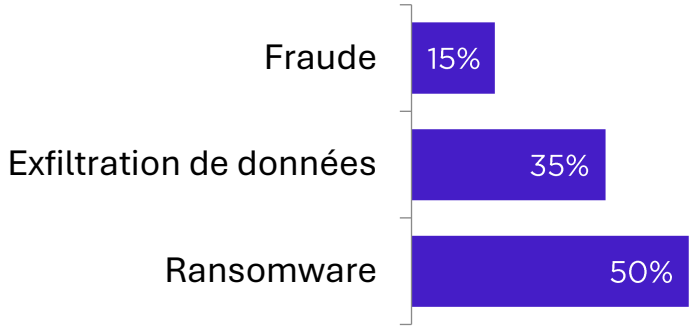
Les gains financiers, principale motivation des attaquants

Les ransomwares et l'exfiltration de données restent les leviers prioritaires en 2025

Gains financiers (65%)

Essentiellement par la mise hors service des systèmes d'information, l'extorsion liée à la divulgation de données sensibles ou encore la fraude.

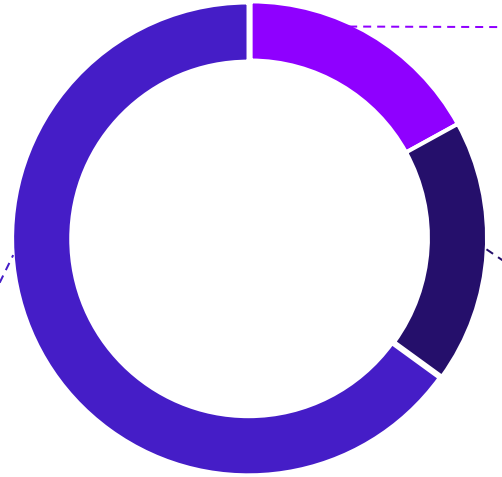
50% en 2024, 46% en 2023



Espionnage (17%)

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

10% en 2024, 8% en 2023



Indéterminées (18%)

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

35% en 2024, 29% en 2023

Cette année, le CERT-Wavestone n'est pas intervenu sur des cas de menaces internes, qui ont été majoritairement traitées par les équipes internes de nos clients.

Ces attaques correspondaient 5% des interventions en 2024, et 6% en 2023.

Le phishing et ses variantes, premier canal d’entrée vers le SI

38%

20% en 2024

Phishing, vishing et utilisation de comptes volés préalablement

Permettant une élévation de privilège en simulant le support informatique ou en compromettant l’ADCS, la CI/CD ou les outils d’hypervision.

22%

20% en 2024

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

Permettant un accès direct aux systèmes critiques de l’entreprise.

20%

40% en 2024

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.

Verbatims des équipes RedTeam Wavestone

« Nos interventions aboutissent de plus en plus fréquemment en passant par des éléments extérieurs au cœur du SI : services Cloud / SaaS, plateforme CI/CD, système d’IAM, etc. »

« Comme l’année dernière, 100% des missions RedTeam ont trouvé des mots de passe stockés dans des espaces de partage. »

Les sauvegardes demeurent une cible de choix…

Comme l'année dernière, l'écrasante majorité des attaques ransomwares ont également vu une compromission des sauvegardes, indispensables en cas de reconstruction. Leur sécurisation reste une priorité pour les DSI.

90%

des attaques ransomwares gérées compromettent également les sauvegardes

Retour terrain : sauvegardes ciblées avant déploiement d’un rançongiciel

Après une intrusion, un attaquant a supprimé les sauvegardes d’un serveur de fichiers avant de télécharger un rançongiciel depuis un dépôt public.

Le malware a été exécuté sur trois serveurs Synology, entraînant le chiffrement des données, bien qu’une tentative ait échoué sur l’un des serveurs.

… tout comme la compromission des données métiers

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. La surveillance et la protection de ces données restent un challenge pour le futur.

71%

des attaques traitées ont comporté un vol de données avéré

Retour terrain : exfiltration de données métiers vers le dark web

Une injection SQL sur une application web a permis le dépôt d’un webshell, offrant à l’attaquant un accès direct aux systèmes internes.

Il a ensuite exfiltré des données personnelles depuis la base de données et le système de fichiers, avant de publier ces informations sensibles sur le dark web.

Des impacts toujours plus rapides après l’intrusion initiale

Les capacités de détection et de réaction des entreprises sont donc davantage mises à l'épreuve, et doivent se tourner aujourd'hui vers davantage d'automatisation, notamment avec l'IA, pour s'adapter à cette accélération.

1,5 jours

est le plus court délai observé entre l’intrusion et l’impact de l’attaque

Retour terrain : une attaque éclair de type ransomware

Grâce à l’exploitation d’un VPN resté accessible avec un compte par défaut, un attaquant a pu s’introduire dans le SI.

Puis, en moins de 24 h, il a pris le contrôle d’un compte administrateur de domaine, exfiltré des données sensibles puis lancé le chiffrement du SI et de ses sauvegardes.

Il a ensuite publié les informations volées sur le dark web.

Les filiales et partenaires utilisés comme porte d’entrée

Malgré des progrès notables en interne dans les grandes entreprises, les filiales et prestataires moins matures demeurent des portes d’entrée privilégiées pour les attaquants. Leur sécurisation à l’échelle reste un challenge.

56%

des attaques visant les grandes entreprises passent par les filiales ou partenaires

Retour terrain : compromission d’un partenaire et fraude financière

Suite au vol d’un compte d’un partenaire par phishing, l’attaquant a eu accès à sa messagerie et aux échanges internes.

L’attaquant a ensuite diffusé de faux RIB par email, utilisant du typosquatting pour se faire passer pour un client légitime et détourner les paiements.

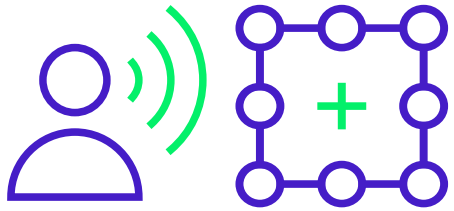
1 Les mutations du phishing

En 2025, les attaquants combinent innovation et social engineering pour renforcer leurs attaques.

Vishing

Les appels vocaux, renforcés parfois par des deepfakes, se multiplient. Perçus comme plus authentiques qu'un mail, ils exploitent souvent l'urgence pour tromper. Une campagne de ce type a ainsi touché des utilisateurs Salesforce durant l'été 2025.

Les équipes financières, administratives mais aussi les supports IT restent les plus ciblées.



Quishing

Cette technique émergente exploite des QR codes piégés par les attaquants. Les victimes scannent un code (ex. via la surcharge d'un sticker légitime ou mis sur un faux document) contenant un lien les redirigeant vers un site ou un contenu frauduleux.

Le quishing, en particulier en environnement ouvert, brouille les repères de l'utilisateur et contourne les filtres traditionnels.

Recommandations principales

Sensibiliser les employés ou les clients qui, en l'absence de mécanisme de protection technique fiable, restent le premier rempart.

Faire évoluer les processus pour éviter une réalisation trop facile des attaques: surveillance des comptes métiers à privilège, renforcement des procédures helpdesk, etc.

Renforcer la détection, et prévoir une **capacité de remontée d'alerte** de la part des utilisateurs et des clients.

2 Les environnements SaaS, nouvelles cibles privilégiées

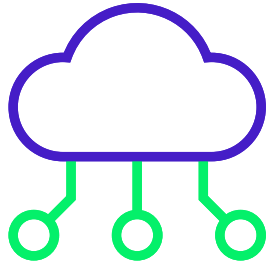
En 2025, les applications collaboratives et services cloud deviennent des portes d'entrée pour les attaquants.

Compromission et abus des API

Les identifiants volés restent le premier point d'entrée vers les comptes SaaS.

Les API et applications tierces mal sécurisées sont aussi exploitées pour exfiltrer fichiers et mails.

Une fois compromis, ils permettent l'accès direct aux données métiers.



Salesforce, une cible privilégiée

Les récentes attaques montrent l'intérêt pour les données contenus dans les CRM.

API mal configurées et détournement de comptes en font une cible pour l'espionnage et la fraude.

Salesforce illustre la valeur stratégique des CRM SaaS pour les attaquants.

Recommandations principales

Imposer le MFA ou des techniques complémentaires sur tous les comptes SaaS sensibles (métiers/IT).

Auditer et contrôler régulièrement les API exposées et intégrations tierces.

Surveiller en continu les accès et comportements inhabituels sur ces environnements.

3 Le piégeage de la supply chain logicielle

Un risque constant et complexe à surveiller.

Vol de cryptomonnaies grâce à des packages open-source compromis

Début septembre 2025, la compromission de 18 packages npm a été révélée. Du code malveillant avait été injecté dans ces composants open-source largement utilisés dans le développement d'application, afin de permettre le vol de cryptomonnaies.

Du code externe, non vérifié, peut rapidement se retrouver sur des plateformes en production.

Transformation massive de packages open-source en chevaux de Troie

Quelques semaines plus tard, une attaque similaire, Shai-Hulud, a compromis plus de 500 paquets npm. Un ver s'est propagé en volant des jetons et clés API de mainteneurs, puis en injectant du code malveillant dans d'autres projets.

Shai-Hulud démontre comment une seule compromission peut contaminer rapidement tout l'écosystème open-source.

Recommandations principales

Cartographier les dépendances logicielles des applications et utiliser des outils de Software Composition Analysis.

Vérifier et mettre à jour régulièrement les paquets tiers depuis des sources fiables et maintenir son propre dépôt.

Mettre en place des plans de réponse spécifiques aux incidents liés à la supply chain logicielle.

Encadrer développeurs externes avec des processus bien définis, des contrôles d'accès stricts et une supervision renforcée.

4 Des attaques amplifiées par l'IA de plus en plus performantes

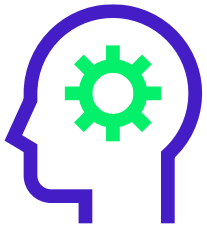
Demandant une adaptation des mécanismes de défense.

Phishing & Deepfakes

Le phishing évolue avec des campagnes massives, multilingues générées par IA.

Les deepfakes vocaux et visuels sont fait pour imiter les dirigeants ou le support IT et sont réalisées maintenant très simplement.

Phishing et deepfakes, amplifiés par l'IA, induisent plus facilement les gens en erreur.



Automatisation de malwares

Au-delà du développement, l'IA est également utilisée dans le fonctionnement de malware.

Par exemple, PromptLock est un ransomware automatisant ses opérations avec l'IA générative: il peut produire des scripts malicieux, et déterminer s'il doit exfiltrer ou chiffrer les données.

Les malwares utilisant l'IA sont plus évolutifs, personnalisés et disposent de capacités plus nombreuses.

Recommandations principales

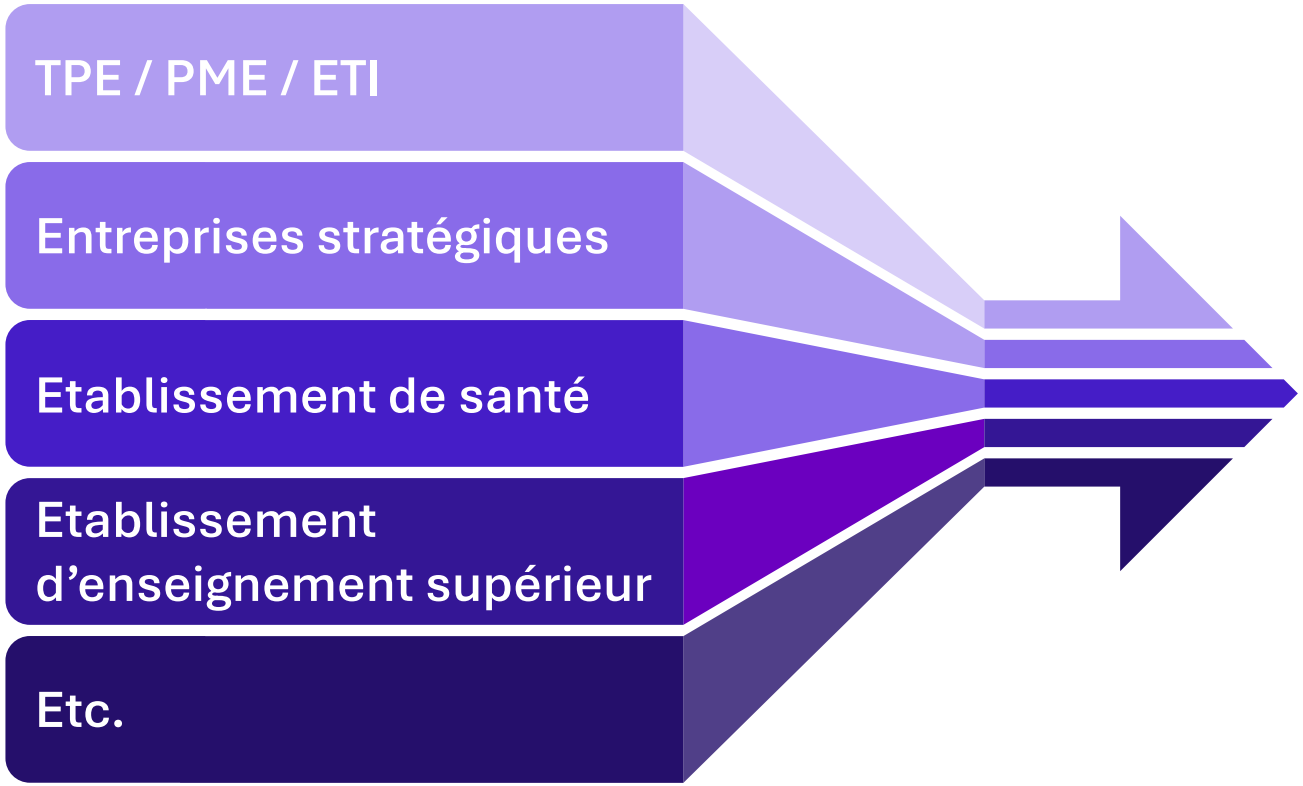
Intégrer des deepfakes dans les **exercices de crise** et dans les **sensibilisations** pour entraîner les équipes.

Mettre en place une détection comportementale des fraudes pour assurer une surveillance en continu.

Automatiser la détection et la réponse pour gagner en réactivité, notamment en s'appuyant sur l'IA au sein des SOC.

Tester les 1ères solutions d'anti-deepfake, le marché commençant à proposer des options matures.

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



21 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 1 500 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

Quentin PERCEVAL
Responsable du CERT-Wavestone
quentin.perceval@wavestone.com