SOPHOS

L'ÉTAT DES RANSOMWARES EN FRANCE 2025

Résultats d'une enquête indépendante menée auprès de 185 entreprises françaises victimes d'une attaque de ransomware au cours de l'année passée.

UN LIVRE BLANC SOPHOS - JUIN 2025

À propos du présent rapport

Ce rapport s'appuie sur les résultats d'une enquête indépendante menée auprès de 3 400 responsables informatiques/cybersécurité travaillant dans des entreprises qui ont été victimes d'un ransomware l'année dernière, dont 185 en France.

L'enquête a été commandée par Sophos et réalisée par un spécialiste indépendant entre janvier et mars 2025.

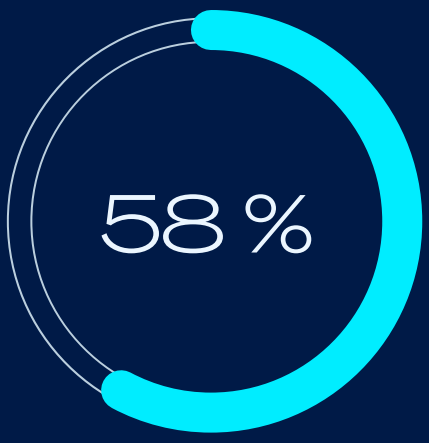
Tous les répondants travaillent au moment de l'enquête dans des organisations comptant entre 100 et 5 000 employés et ont été invités à répondre en se basant sur leur expérience au cours des 12 derniers mois.

Le rapport comprend des comparaisons avec les résultats de notre enquête de 2024. Toutes les données financières sont exprimées en dollars américains.

Enquête auprès de

185

Responsables informatiques/cybersécurité en France travaillant dans des organisations qui ont été victimes d'un ransomware au cours de l'année écoulée



Pourcentage d'attaques ayant abouti au chiffrement des données.

Le montant médian des rançons payées en France l'année dernière.

Le coût moyen de rétablissement après une attaque de ransomware.

Pourquoi les entreprises françaises sont-elles victimes de ransomware

- **L'exploitation de vulnérabilités est la cause première technique** la plus fréquemment citée, utilisée dans 30 % des incidents. Elle est suivie par les emails malveillants, qui ont été à l'origine de 24 % des attaques. Dans 23 % des attaques, ce sont des identifiants compromis qui ont été utilisés.
- **Une faille de sécurité connue était la cause première opérationnelle la plus fréquente**, citée par 43 % des répondants français. Venaient ensuite le manque d'expertise et une erreur humaine, cités tous deux par 42 % des entreprises.

Ce qu'il advient des données

- **58 % des attaques sont parvenues à chiffrer des données.** Ce chiffre est supérieur à la moyenne mondiale de 50 %, mais représente une baisse significative par rapport aux 87 % déclarés par les répondants français en 2024.
- **Des données ont été volées dans 44 % des attaques où des données ont été chiffrées**, soit plus du double des 20 % signalés l'année dernière.
- **98 % des entreprises françaises dont les données ont été chiffrées ont pu les récupérer,** soit un peu plus que la moyenne mondiale.
- **33 % des entreprises françaises ont payé la rançon et récupéré leurs données,** soit une baisse significative par rapport aux 60 % de l'année dernière.
- **60 % des entreprises françaises ont utilisé des sauvegardes pour récupérer leurs données chiffrées,** soit une baisse par rapport aux 70 % de l'année dernière.

Rançons : montants demandés et montants payés

- **Le montant médian des demandes de rançon en France l'année dernière s'élevait à 643 125 dollars,** ce qui représente une baisse considérable par rapport aux 4,72 millions de dollars rapportés dans notre enquête de 2024.

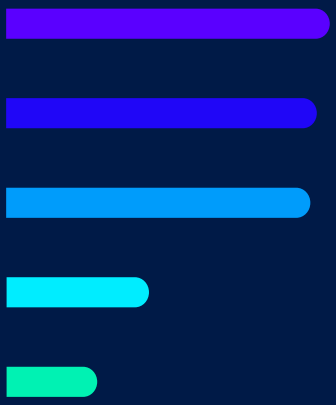
Le montant médian de la demande de rançon en France l'année dernière.

- **49 % des demandes de rançon s'élevaient à 1 million de dollars ou plus,** contre 79 % en 2024.
- **Le montant médian des rançons versées en France l'année dernière était de 231 525 dollars,** soit une baisse considérable par rapport aux 7,08 millions de dollars signalés l'année dernière.
- **Les entreprises françaises ont généralement payé 87 % du montant de la rançon demandée,** soit légèrement moins que la moyenne mondiale de 85 %.
  - 38 % **ont payé MOINS que la rançon initialement** demandée (moyenne mondiale : 53 %).
  - 50 % **ont payé LE MÊME MONTANT que la rançon initialement demandée** (moyenne mondiale : 29 %).
  - 12 % **ont payé PLUS que la rançon initialement** demandée (moyenne mondiale : 18 %).

L'impact économique des ransomwares

- Si l'on exclut le paiement des rançons, **la facture moyenne supportée par les entreprises françaises pour se remettre d'une attaque de ransomware au cours de l'année écoulée s'est élevée à 1,22 million de dollars,** soit une baisse substantielle par rapport aux 3,27 millions de dollars déclarés par les répondants français en 2024. Cette somme comprend les coûts liés aux interruptions de services, le temps passé à la résolution de l'incident, les coûts matériels, les pertes d'exploitation, etc.
- **Les entreprises françaises se remettent de plus en plus rapidement d'une attaque de ransomware :** 53 % d'entre elles ont entièrement récupéré leurs données en moins d'une semaine, ce qui représente une augmentation significative par rapport aux 16 % de l'année dernière. 18 % ont mis entre un et six mois pour récupérer leurs données, ce qui représente une baisse notable par rapport aux 58 % de l'année dernière.

L'impact humain des ransomwares sur les équipes informatiques/ cybersécurité des entreprises dont les données ont été chiffrées



50 % font état d'une **augmentation de leur anxiété ou de leur stress** face à de futures attaques.

48 % déclarent que **la charge de travail de l'équipe a augmenté** depuis l'attaque.

47 % **se sentent coupables** de ne pas avoir pu empêcher l'attaque.

22 % ont connu **l'absence d'un membre de leur équipe** pour cause de stress ou de problèmes de santé mentale.

14 % indiquent que **la direction de l'équipe a été remplacée**.

Recommandations

Les ransomwares restent une menace majeure pour les entreprises françaises. Tandis que les adversaires continuent de multiplier et de faire évoluer leurs attaques, il est essentiel que les défenseurs ne soient pas pris de vitesse et que leurs cyberdéfenses évoluent en conséquence. Les enseignements tirés de ce rapport indiquent les domaines clés sur lesquels il faudra se concentrer en 2025 et au-delà.

- **Prévention.** Une bonne attaque de ransomware est une attaque qui n'a pas eu lieu, car les adversaires n'ont pas réussi à pénétrer votre entreprise. Cherchez à réduire à la fois les causes techniques et les causes opérationnelles des attaques mises en évidence dans ce rapport.
- **Protection.** Il est impératif de disposer d'outils de sécurité de base performants. Les systèmes endpoint (dont les serveurs) sont la cible principale des auteurs de ransomwares, c'est pourquoi il faut vous assurer que ceux-ci sont bien protégés, y compris par une protection anti-ransomware dédiée pour bloquer et annuler tout processus de chiffrement malveillant.
- **Détection et réponse.** Pour assurer une issue plus favorable, il est essentiel de stopper une attaque le plus tôt possible. Un service de détection et de réponse aux menaces fonctionnant 24 heures sur 24 constitue désormais une couche de défense essentielle. Si vous ne disposez pas des ressources ou des spécialistes nécessaires pour mettre en place cette solution en interne, envisagez de faire appel à un fournisseur de services MDR (Managed Detection and Response) de confiance.
- **Planification et préparation.** En disposant d'un plan de réponse aux incidents que vous savez parfaitement mettre en œuvre, vous améliorerez considérablement vos résultats si le pire se produit et que vous êtes victime d'une attaque de grande ampleur. Veillez à effectuer des sauvegardes régulières et à vous entraîner régulièrement à les restaurer.

SOPHOS

Pour découvrir comment Sophos peut vous aider à optimiser vos défenses contre les ransomwares, contactez un conseiller ou visitez le site **www.sophos.fr/ransomware2025**

Sophos fournit des solutions de cybersécurité de pointe aux entreprises de toutes tailles, les protégeant en temps réel contre les menaces avancées telles que les malwares, les ransomwares et le phishing. Grâce à des fonctionnalités Next-Gen éprouvées, les données de votre entreprise sont sécurisées efficacement par des produits alimentés par l'intelligence artificielle et le Machine Learning.

2025-07-09 FR-WP (DD)