SOPHOS

L'ÉTAT DES RANSOMWARES EN FRANCE 2026

Résultats d'une enquête indépendante, sans parti pris envers les éditeurs, menée auprès de 129 organisations françaises victimes d'une attaque de ransomware au cours de l'année passée.

LIVRE BLANC SOPHOS - JUILLET 2026

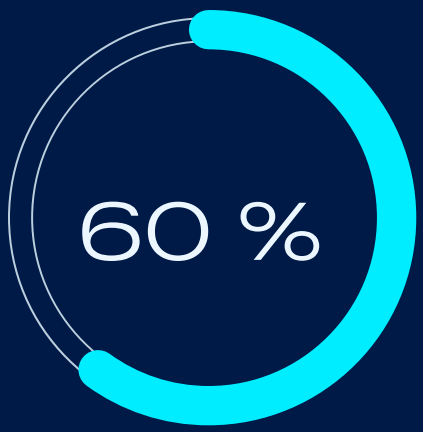
À propos du présent rapport

Ce septième rapport annuel sur l'état des ransomwares s'appuie sur les résultats d'une enquête indépendante, commandée par Sophos. Le rapport de cette année s'appuie sur les résultats d'une enquête indépendante menée auprès de 2 158 responsables informatiques/cybersécurité travaillant dans des entreprises qui ont été victimes d'un ransomware l'année dernière, dont 129 en France.

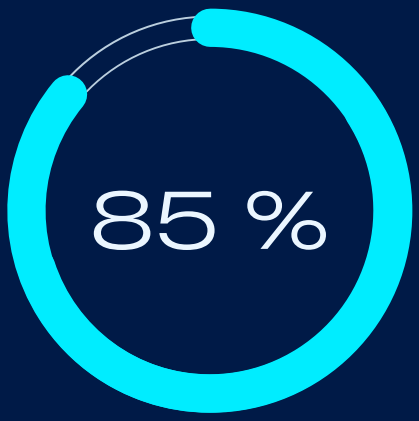
L'enquête a été menée entre janvier et mars 2026. Tous les répondants travaillent au moment de l'enquête dans des organisations comptant entre 100 et 5 000 employés et ont été invités à répondre en se basant sur leur expérience au cours des 12 derniers mois. Toutes les données financières sont exprimées en dollars américains. les rançons aberrantes de 40 millions de dollars ou plus ont été supprimées de ces données.

Enquête auprès de 129

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.



Ont confirmé que l'incident de ransomware de l'année dernière était le même événement que leur attaque d'identité la plus importante.

Le coût moyen de rétablissement après une attaque de ransomware.

Pourquoi les entreprises françaises sont-elles victimes de ransomware

- **Les identifiants compromis étaient la cause première technique la plus fréquente des attaques,** utilisés dans 30 % des attaques, suivis par le phishing (27 %) et les emails malveillants (20 %). Les vulnérabilités exploitées ont fortement diminué, tombant à 13 % contre 30 % dans le rapport 2025.
- **(NOUVEAU) 85 % ont confirmé que l'incident de ransomware de l'année dernière était le même événement que leur attaque d'identité la plus importante.** Ce chiffre est nettement supérieur à la moyenne mondiale de 67 %.
- **(NOUVEAU) Les applications et les systèmes exposés étaient le point d'entrée des attaques le plus courant (46 %)** pour les causes racines non liées aux email et au phishing, suivis des appareils utilisateurs (22 %) et des VPN (15 %). La France a le pourcentage le plus élevé de points d'entrée d'attaques liés aux VPN parmi tous les pays étudiés.
- **Le manque de personnel/de capacités (40 %) est la cause racine opérationnelle la plus fréquente,** suivi par le manque de protection (38 %) et le manque d'expertise (33 %).

Ce qu'il advient des données

- **60 % des attaques ont abouti au chiffrement des données.** Ce chiffre est supérieur à la moyenne mondiale de 56 %, et représente une hausse significative par rapport aux 58 % déclarés par les répondants français en 2025.
- **Des données ont également été volées dans 18 % des attaques ayant abouti à un chiffrement,** une baisse considérable par rapport aux 44 % signalés en 2025.
- **100 % des organisations françaises dont les données ont été chiffrées ont pu les récupérer,** conformément à la moyenne mondiale.
- **36 % des organisations françaises ont payé la rançon et récupéré leurs données,** soit une légère augmentation par rapport aux 33 % de l'année dernière.
- **76 % des organisations françaises ont utilisé des sauvegardes pour récupérer leurs données chiffrées,** soit une augmentation considérable par rapport aux 60 % signalés dans le rapport 2025.

Les demandes de rançon

Montant médian de la demande de rançon en France.

- **Le montant médian des rançons demandées en France s'élevait à 500 000 dollars,** soit 22 % de moins que les 643 125 dollars déclarés dans le rapport 2025.
  - **39 % des demandes de rançon s'élevaient à 1 million de dollars ou plus,** un chiffre en baisse par rapport aux 49 % signalés dans le rapport 2025.

L'impact économique des ransomwares

- En excluant le paiement de la rançon, **le coût moyen encouru par les organisations françaises pour se remettre d'une attaque de ransomware dans le rapport de cette année s'élève à 2,02 millions de dollars,** soit une augmentation significative par rapport à la moyenne de 1,22 million de dollars signalée dans le rapport 2025. Cette somme comprend les coûts liés aux interruptions de services, le temps nécessaire à la résolution de l'incident, les coûts matériels, les pertes d'exploitation, etc.
- **64 % des organisations françaises se sont remises d'une attaque de ransomware en une semaine ou moins,** une augmentation considérable par rapport aux 53 % signalés dans le rapport 2025. 10 % ont mis entre un et six mois pour récupérer leurs données, ce qui représente une baisse notable par rapport aux 18 % relevé dans le rapport 2025.

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

42 % signalent une pression accrue de la part des hauts dirigeants.

37 % signalent une reconnaissance accrue de la part des cadres supérieurs. En hausse par rapport aux 18 % de 2025

33 % signalent une augmentation continue de la charge de travail depuis l'attaque.

31 % se sentent coupables de ne pas avoir pu empêcher l'attaque.

17 % ont indiqué que la direction de l'équipe a été remplacée.

Recommandations

Renforcez la sécurité des identités pour vous prémunir contre les ransomwares. La grande majorité des victimes françaises de ransomware ont confirmé que leur incident de ransomware correspondait également à que leur attaque d'identité la plus grave. Les organisations doivent accorder la priorité à la détection et à la réponse aux menaces liées aux identités (ITDR), appliquer une authentification multifacteur sur tous les points d'accès et auditer régulièrement les identifiants des identités humaines et non humaines.

Renforcez la protection Endpoint pour les modèles d'IA frontière. L'IA frontière accélère la découverte et l'exploitabilité des vulnérabilités. Il est essentiel de disposer de défenses Endpoint solides qui bloquent automatiquement les attaques basées sur des exploits.

Priorisez la sécurité des messageries. Le phishing et les emails malveillants représentent près de la moitié des causes premières des ransomwares en France. Les organisations devraient déployer un filtrage avancé des emails, implémenter les protocoles DMARC/ DKIM/SPF et investir dans des formations régulières de sensibilisation au phishing.

Investissez dans une infrastructure de sauvegarde et de restauration. Les organisations ayant maintenu des systèmes de sauvegarde robustes ont récupéré des données chiffrées à un rythme presque record au cours de l'année écoulée. Les sauvegardes doivent être testées régulièrement, stockées hors ligne ou dans des formats immuables, et intégrées dans un plan de réponse aux incidents documenté pouvant être exécuté sous pression.

SOPHOS

Pour découvrir comment Sophos peut vous aider à optimiser vos défenses contre les ransomwares, contactez un conseiller ou visitez **sophos.com/ransomware2026**

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.

2026-08-03 FR-WP (TA) CRE-6006