



LES ATTAQUES PAR RANSOMWARE
AUGMENTENT POUR LA PREMIÈRE
FOIS DEPUIS TROIS ANS



RANSOMWARE IMPACT

REPORT 2025



RAPPORT D'ENQUÊTE HORNETSECURITY SUR L'IMPACT DES RANSOMWARES EN 2025

Après avoir observé une baisse du nombre d'attaques au cours des dernières années, les ransomwares sont de nouveau en hausse. En 2025, **24 %** des organisations ont déclaré avoir été victimes d'une attaque par ransomware, soit **une forte augmentation par rapport aux 18,6 % enregistrés en 2024**, marquant ainsi la fin d'une tendance à la baisse qui durait depuis de nombreuses années. Alors que de plus en plus d'entreprises mettent en place des mesures de protection, les pirates diversifient leurs méthodes et exploitent les nouvelles technologies telles que l'IA pour contourner les défenses traditionnelles.



HORNETSECURITY

- » **13 %** des victimes de ransomware ont payé la rançon, contre 16,3 % en 2024, ce qui témoigne d'une réticence croissante, ou d'une meilleure préparation, à ne pas négocier.
- » **74 %** des organisations forment leurs employés à reconnaître et à prévenir les ransomwares, bien que 42 % d'entre elles estiment que la formation est encore insuffisante ou trop superficielle.
- » **26 %** des incidents liés au ransomware ont impliqué des terminaux compromis, ce qui reflète l'exploitation croissante des environnements de travail à distance et des appareils non mis à jour.
- » **77 %** des personnes interrogées considèrent le phishing basé sur l'IA comme une menace sérieuse et émergente.
- » **46 %** des attaques étaient toujours liées au phishing, mais cela représente une baisse par rapport aux 52,3 % enregistrés en 2024, les auteurs de menaces explorant d'autres points d'entrée tels que le vol d'identifiants et les exploits zero-day.
- » **46 %** des organisations ont souscrit une assurance contre les ransomwares, contre 54,6 % en 2024, peut-être en raison de l'augmentation des primes, des exclusions ou d'une confiance réduite dans les remboursements.
- » **62 %** des organisations utilisent désormais des sauvegardes immuables, ce qui suggère une meilleure préparation et des capacités de récupération améliorées.
- » **82 %** ont mis en place un plan de reprise après sinistre, qui pourrait devenir une nouvelle norme en matière de résilience.

LA SITUATION EN 2025

Les ransomwares continuent d'évoluer et, en 2025, ils ne font pas que persister, ils connaissent un regain d'activité. Pour rester informé des dernières évolutions en matière de ransomware, l'équipe Hornetsecurity mène régulièrement des enquêtes internationales afin de suivre les tendances et de recueillir les avis des professionnels de l'informatique.

Comptant parmi les menaces les plus perturbatrices pour les organisations du monde entier, les ransomwares ont réaffirmé leur présence avec une sophistication et une portée accrue. Les préoccupations liées à la cybersécurité en général sont de plus en plus vives. **76 % des responsables de la sécurité estiment qu'une cyberattaque majeure est probable dans les 12 prochains mois ; cette perception a fortement augmenté, faisant écho à la résurgence des attaques identifiées dans notre rapport.**

Les résultats de cette année montrent un renversement brutal de la tendance à la baisse de la fréquence des attaques, soulignant à la fois l'ampleur croissante des opérations de ransomware et le besoin urgent de mettre à jour les défenses. En 2024, seuls 18,6 % des répondants ont déclaré avoir été victimes d'une attaque de ransomware, le chiffre le plus bas depuis 2021. Mais cette année, ce chiffre est remonté à 24 %, soulignant une résurgence inquiétante de l'activité des ransomwares.

Cette augmentation semble être due à deux facteurs clés : une plus grande automatisation des attaques et un éventail plus large de tactiques utilisées par les cybercriminels. Si le phishing traditionnel reste le principal vecteur d'attaque (signalé par 46 % des personnes interrogées), les données montrent un recours croissant aux terminaux compromis (26 %) et aux identifiants volés, souvent liés à de mauvaises pratiques de correction et à des environnements « Bring Your Own Device (BYOD) ».

Malgré l'augmentation du volume des attaques, moins d'entreprises paient les rançons, ce qui suggère une meilleure préparation à la reprise ou une réticence croissante à traiter avec les extorqueurs. Cependant, l'impact financier et opérationnel des attaques reste grave, d'autant plus que les ransomwares deviennent plus ciblés et persistants.

Les ransomwares sont des logiciels malveillants très destructeurs qui verrouillent l'accès des entreprises à leurs données et à leurs systèmes, les auteurs des menaces exigeant un paiement, souvent en cryptomonnaie, en échange de la restauration. Les conséquences peuvent inclure la perte de données, des temps d'arrêt, des sanctions réglementaires et une atteinte à la réputation. Selon le rapport 2025 Proofpoint Voice of the CISO, 66 % des entreprises ont récemment subi une perte de données sensibles. Ce chiffre, nettement supérieur à celui de l'année dernière, souligne la nécessité de renforcer la résilience, comme nous l'avons évoqué dans notre étude. En outre, 58 % des RSSI estiment qu'ils ne sont pas suffisamment préparés aux cybermenaces, malgré la mise en place généralisée de plans de reprise après sinistre.

Cette année, les personnes interrogées ont également donné un aperçu de l'évolution de leurs stratégies en matière de cybersécurité. Les investissements dans les outils de détection des terminaux, les sauvegardes régulières et la formation des utilisateurs restent les piliers essentiels de la défense contre les ransomwares. Mais avec l'augmentation des attaques basées sur les identifiants et les exploits logiciels, les résultats soulignent l'importance d'adopter des architectures de sécurité multicouches et des principes de confiance zéro.

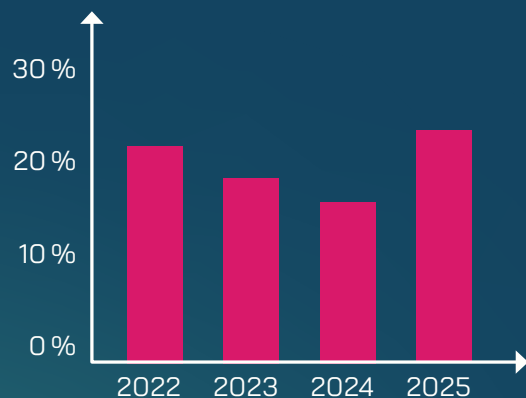
Alors que les tactiques des ransomwares deviennent plus complexes et multifacettes, les organisations doivent garder une longueur d'avance, non seulement en se défendant contre les attaques initiales non seulement en se défendant contre les premières violations, mais aussi en mettant en place des systèmes résilients capables de se rétablir rapidement en cas d'incident.

„58 % des RSSI estiment qu'ils ne sont pas suffisamment préparés aux cybermenaces.“



LES ATTAQUES PAR USURPATION D'IDENTITÉ SE MULTIPLIENT TOUT AUTANT QUE LES RANSOMWARES

Après plusieurs années de baisse du nombre de victimes, l'année 2025 marque une nette recrudescence des ransomwares. Cette année, 24 % des entreprises ont déclaré avoir été victimes d'une attaque par ransomware, soit une forte augmentation par rapport aux 18,6 % enregistrés en 2024, inversant ainsi la tendance à la baisse observée depuis 2021.



Pourcentage d'entreprises interrogées touchées par un ransomware

Cette nouvelle augmentation est étroitement liée à l'adoption par les attaquants de méthodes plus automatisées et améliorées par l'IA, qui leur permettent d'étendre leurs opérations tout en conservant leur précision. La sophistication continue de s'accroître, en particulier en ce qui concerne la manière dont les attaquants identifient et exploitent les vulnérabilités des environnements informatiques hybrides.

Il est intéressant de noter que, même si moins de victimes paient des rançons, avec seulement 13 % déclarant avoir payé pour récupérer leurs données, contre 16,3 % en 2024, l'impact global reste important. Les attaquants provoquent des perturbations généralisées, utilisant l'exfiltration et la destruction de données comme moyen de pression, même lorsque les paiements ne sont pas effectués.

L'IA AMPLIFIE LES CYBERMENACES

L'une des caractéristiques marquantes des ransomwares cette année est l'intégration croissante des outils d'IA dans les stratégies d'attaque. Comme le souligne le rapport Proofpoint Voice of the CISO 2025, l'adoption croissante de l'IA générative et des outils collaboratifs expose les entreprises à de nouveaux risques : 60 % des RSSI considèrent l'IA générative comme une menace pour la sécurité, et 68 % investissent dans des capacités de détection et de protection basées sur l'IA. De plus :

- » **77 % des RSSI interrogés ont identifié le phishing généré par l'IA comme une menace réelle et croissante.**
- » **61 % estiment que l'IA a considérablement accru le risque global d'attaques par ransomware.**

Les pirates utilisent désormais l'IA générative pour créer :

- » Des emails de phishing hautement personnalisés,
- » Des fichiers audio et vidéo deepfake à des fins d'ingénierie sociale,
- » Des stratégies d'intrusion automatisées et multivectorielles.

Ce niveau d'automatisation et de tromperie a rendu les méthodes de détection traditionnelles moins efficaces, nécessitant une transition vers des plateformes EDR/XDR, des cadres zero-trust et la détection automatisée des anomalies.

„77% des RSSI interrogés ont identifié le phishing généré par l'IA comme une menace réelle et croissante.”

CHANGEMENT DES POINTS D'ENTRÉE : AU-DELÀ DU PHISHING

Si le phishing reste le principal vecteur d'accès initial, sa prédominance s'estompe légèrement. Cette année :

- » Les attaques par e-mail de phishing ont chuté à **46 %** (contre **52,3 % en 2024**),
- » Les terminaux compromis représentent désormais **26 %** des livraisons de ransomware,
- » Les identifiants volés ont été impliqués dans environ **25 %** des attaques,
- » Les vulnérabilités exploitées ont contribué à **12 %**.

Ces changements mettent en évidence un changement stratégique de la part des acteurs malveillants, qui ciblent les organisations où l'authentification multifactorielle (MFA) est faible, les correctifs sont incohérents et le shadow IT reste omniprésent, en particulier dans les environnements de travail à distance et hybrides.

LACUNES EN MATIÈRE DE FORMATION ET « FAUSSE CONFORMITÉ »

Bien que **74 %** des organisations déclarent proposer des formations aux utilisateurs finaux contre les ransomwares, **42 %** des responsables de la sécurité admettent que leurs formations sont insuffisantes ou inefficaces.

Ce décalage a donné lieu à un phénomène inquiétant : la « fausse conformité », qui consiste pour les organisations à respecter des normes de sensibilisation superficielles sans pour autant s'engager de manière significative ni mettre en œuvre les meilleures pratiques.

Les petites et moyennes entreprises (PME) sont particulièrement exposées à ce risque, car elles organisent souvent des sessions de formation annuelles de type « checklist » sans véritable suivi. Cela contribue à la persistance des erreurs humaines en tant que vulnérabilité, en particulier face aux tactiques avancées de phishing et d'ingénierie sociale. Selon Proofpoint, l'erreur humaine reste la principale source d'incidents : **66 %** des RSSI identifient le facteur humain comme le risque principal, en particulier en termes de fuites de données et de compromission interne. Bien que la formation s'améliore, elle reste souvent superficielle (42 % la jugent inadéquate). Ces résultats corroborent les conclusions de Hornetsecurity sur les limites des programmes de « conformité à cocher ».

LA RÉSILIENCE ÉGALEMENT EN HAUSSE : PROTECTION, PLANS ET REPRISE

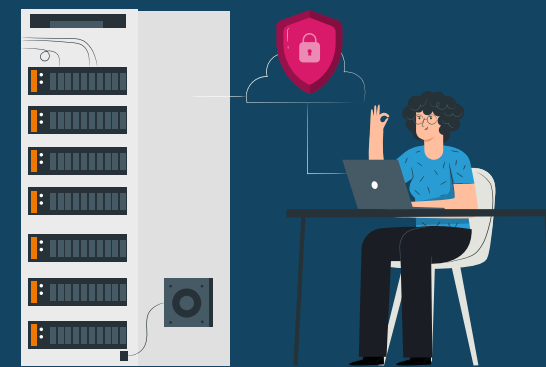
Malgré l'évolution du paysage des menaces, tout n'est pas sombre. Des signes d'amélioration de la préparation et de la maturité opérationnelle apparaissent à tous les niveaux :

- » **82 %** des organisations ont désormais mis en place un plan de reprise après sinistre (DR), une étape importante qui suggère que la planification de la reprise après sinistre devient une attente de base.

- » **62 %** ont adopté des sauvegardes immuables, qui ne peuvent être modifiées ou cryptées, même pendant une attaque active.

Ces mesures semblent porter leurs fruits : si le nombre de victimes de ransomware est en hausse, la proportion de victimes payant une rançon est en baisse, ce qui suggère que les capacités de reprise et la préparation aux menaces s'améliorent.

Il existe toutefois une nuance cruciale : les pertes de données et les perturbations opérationnelles restent élevées, en particulier parmi les petites organisations, qui manquent encore souvent de sauvegardes segmentées, d'équipes d'intervention en cas d'incident ou de protocoles de test de reprise.



LE DÉFICIT DE PRÉPARATION DES PME

Les petites entreprises continuent d'être confrontées à des risques disproportionnés :

- » Elles représentent une part disproportionnée des victimes,
- » Beaucoup d'entre elles disposent d'un personnel informatique minimal, d'une infrastructure obsolète ou font appel à des prestataires externes dont les compétences sont limitées,
- » Les formations sont souvent peu fréquentes ou trop génériques,
- » Le shadow IT et les mauvaises pratiques en matière de correctifs sont monnaie courante.

Bien que davantage de PME déclarent désormais disposer d'un plan de reprise après sinistre, nos données suggèrent que la « préparation » sur le papier ne se traduit pas toujours par une résilience réelle en cas d'attaque.

Les organisations qui se conforment à la norme ISO 27001 ou à des cadres de conformité similaires obtiennent de meilleurs résultats, mais beaucoup confondent encore certification et maturité en matière de sécurité, une distinction essentielle.

SEULEMENT 13 % DES VICTIMES ONT PAYÉ, MAIS LA MENACE PERSISTE

Cette année, 13 % des victimes ont déclaré avoir payé une rançon, contre 16,3 % en 2024. Cela suggère que davantage d'organisations se remettent de l'attaque sans céder, grâce à :

- » Une meilleure maturité des sauvegardes, telles que les sauvegardes immuables (protection directe contre les ransomwares),
- » Une adoption plus large des plans de reprise après sinistre (DR),
- » Des protocoles de réponse plus clairs.

Cependant, la menace elle-même ne diminue pas, elle change de forme. La double extorsion, l'exfiltration ciblée de données et le sabotage de la réputation font désormais partie intégrante des stratégies des attaquants. Et même si moins de rançons sont payées, les dommages financiers restent importants en raison des temps d'arrêt, de la perte de données et des frais de récupération.

De plus, nous avons observé une baisse de l'adoption des assurances contre les ransomwares :

- » **46 %** des organisations déclarent avoir souscrit une assurance contre les ransomwares en 2025, contre **54,6 %** en 2024.
- » Les raisons invoquées sont l'augmentation des primes, le durcissement des critères d'éligibilité et la limitation des indemnités versées.

Cette évolution suggère que le recours à l'assurance n'est plus considéré comme un plan de secours, ce qui souligne encore davantage la nécessité de disposer de défenses internes solides.

„Cette année, 13 % des victimes ont déclaré avoir payé une rançon, contre 16,3 % en 2024.”



LES ATTAQUES AMÉLIORÉES PAR L'IA STIMULENT L'INNOVATION EN MATIÈRE DE DÉFENSE

Le phishing alimenté par l'IA étant désormais une préoccupation majeure, les organisations réagissent en :

- » Adoptant de plus en plus les plateformes de détection et de réponse étendues (XDR),
- » Évoluant vers des architectures Zéro Trust,
- » Intégrant l'analyse comportementale basée sur l'IA pour détecter les premiers signes d'activité de ransomware.

» Cependant, les attaquants évoluent tout aussi rapidement, utilisant des deepfakes, des leurres créés par l'IA et une automatisation en plusieurs étapes pour pirater les systèmes avec une rapidité et une subtilité sans précédent.

Cette course à l'armement entre les attaquants et les défenseurs basés sur l'IA devrait définir l'évolution des ransomwares au cours des prochaines années.

LEADERSHIP ET GOUVERNANCE : TOUJOURS EN RETARD

La cybersécurité est de plus en plus une question qui relève du conseil d'administration, en raison :

- » De la pression réglementaire croissante (NIS2, DORA, etc.),
- » Du risque croissant pour la réputation liée à la médiatisation des violations,
- » Du lien direct entre les incidents cybernétiques et la continuité des activités.

Pourtant, de nombreuses organisations signalent encore un décalage entre les réalités techniques et la compréhension des dirigeants :

- » Peu de conseils d'administration participent à des simulations de crises cybernétiques,
- » Les manuels interfonctionnels sont rares,
- » Les plans de communication externe, en particulier en cas de désinformation alimentée par l'IA ou d'extorsion basée sur des deepfakes, sont sous-développés.

À mesure que les menaces deviennent plus sophistiquées et que leur impact sur le public augmente, la cyber-gouvernance doit évoluer au-delà de la conformité pour atteindre une préparation stratégique.



INDICATEURS CLÉS : 2024 VS 2025

INDICATEURS	2024	2025
Taux de victimisation	18.6 %	24 %
Attaques par hameçonnage / phishing	52.3 %	46 %
Identifiants compromis	~20 % (est.)	~25 %
Vulnérabilités exploitées	–	~12 %
Rançon versée	16.3 %	13 %
Adoption d'une assurance contre les ransomwares	54.6 %	46 %
Organisations proposant des formations aux utilisateurs	81.3 %	74 %
Formation jugée inadéquate	–	42 %
Sauvegardes immuables	–	62 %
Mise en oeuvre d'un PRA	–	82 %
IA phishing perçu comme une menace	66.9 %	77 %

LA RÉSILIENCE S'AMÉLIORE, MAIS LES MENACES AUSSI

2025 marque un tournant dans le paysage des ransomwares. Bien que le nombre d'attaques et la perception des menaces augmentent, les contre-mesures se multiplient en réponse.

Pour la première fois en trois ans, les attaques sont à nouveau en hausse, touchant jusqu'à **24 %** des organisations, inversant ainsi la tendance à la baisse. Cette résurgence est alimentée par l'automatisation, le phishing amélioré par l'IA et des tactiques de plus en plus ciblées et à plusieurs étapes.

Cependant, nos conclusions révèlent également des progrès encourageants en matière de résilience et de préparation :

- » Les paiements de rançons ont chuté à seulement **13 %**, ce qui indique une plus grande confiance dans la reprise.
- » **62 %** des organisations utilisent des sauvegardes immuables, ce qui représente une augmentation significative par rapport aux années précédentes.
- » **82 %** disposent désormais d'un plan de reprise après sinistre (DR), établissant une nouvelle base de référence en matière de préparation.

Le phishing reste le principal vecteur d'attaque, mais les terminaux compromis et les identifiants volés comblent l'écart.



Les menaces basées sur l'IA sont en augmentation, mais les défenses alimentées par l'IA le sont également.

ET MAINTENANT ?

Les ransomwares deviennent de plus en plus sophistiqués, mais les défenseurs aussi. Pour aller de l'avant, il faut reconnaître que les violations sont inévitables, mais que les dommages ne le sont pas forcément.

Les organisations les plus résilientes passent d'une défense réactive à des stratégies proactives :

- » Renforcement de la protection des terminaux et des identités
- » Test et validation réguliers des systèmes de reprise après sinistre et de sauvegarde
- » Formation continue et réaliste des utilisateurs, et non simple conformité aux normes
- » Mise en oeuvre du modèle Zero Trust et de l'analyse comportementale
- » Réduction de l'écart entre la réponse technique et le leadership exécutif

Pour faire face à ces menaces en constante évolution, 365 Total Protection de Hornetsecurity offre la plus large gamme de fonctionnalités de sécurité Microsoft 365 qui rationalisent et pérennisent vos opérations commerciales.

Développé par des experts en sécurité de confiance, 365 Total Protection s'intègre de manière transparente à Microsoft 365 et offre aux entreprises une technologie de nouvelle génération basée sur l'IA, facile à utiliser et d'une efficacité sans faille dans la lutte contre les ransomwares et autres cybermenaces.

Les ransomwares continuent d'évoluer, votre défense doit en faire autant. **Avec 365 Total Protection, vous ne vous contentez pas de réagir, vous gardez une longueur d'avance.**

365 TOTAL PROTECTION

SUITE COMPLÈTE POUR MICROSOFT 365
SÉCURITÉ, RISQUES, GOUVERNANCE,
CONFORMITÉ ET SAUVEGARDE

EN SAVOIR PLUS

BONJOUR,
JE M'APPELLE AI.MY ! JE SUIS
VOTRE RENFORT EN MATIÈRE
DE SÉCURITÉ IA POUR M365





Département
Commercial



Vous accompagne



HAFS NETWORKS WCA



+225 07 89 82 56 49 / +225 07 59 05 85 82



sales-ci@hafs-networks.com



HAFS NETWORKS FRANCE



+33 (0)7 49 92 62 57 / +33(0)9 73 89 20 39



sales@hafs-networks.com

Distributeur à Valeur Ajoutée de Solutions de Cybersécurité | Réseaux | Wi-Fi | HCI/Sauvegarde

