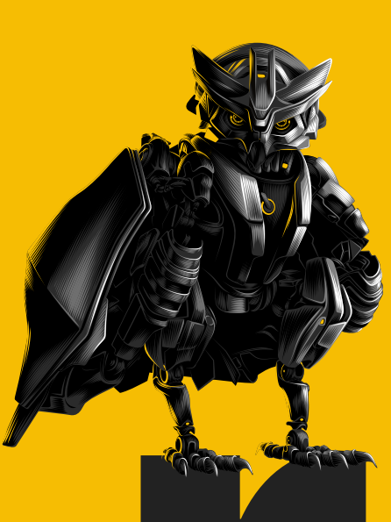
cybereason



Ransomware: Coût réel pour les entreprises françaises en 2024

Résultats de notre étude annuelle sur l'impact des ransomwares.

La France, comme tant d'autres pays non anglophones, connaît une recrudescence des attaques par ransomware. Selon notre étude, 90 % des entreprises concernées ont versé une rançon, mais moins de la moitié d'entre elles ont récupéré un système non corrompu. Par ailleurs, la majorité de ces organisations ont été victime d'une nouvelle attaque quelques mois plus tard.

Des attaques en pleine mutation

Les groupes cyber font appel à l'IA générative pour traduire et adapter leurs attaques aux pays non anglophones. Ils déploient également des méthodes détournées pour pénétrer les réseaux.

43 %

se sont infiltrés via un partenaire de la supply chain

21 %

se sont infiltrés à l'aide d'un acteur interne.

18 %

se sont infiltrés directement.

Que recherchent-ils ?

- **Propriété intellectuelle (PI)/ secrets commerciaux**
- **Identifiants de comptes**
- **Données à caractère personnel**
- **Données médicales personnelles**
- **Données clients**

Payer n'est pas la meilleure solution

Alors que la plupart des victimes acceptent de verser une rançon, **moins de 40 % d'entre elles parviennent à récupérer des systèmes et des données non corrompus**. Par ailleurs, **la majorité de ces entreprises font l'objet d'une nouvelle compromission** dans les six mois.

90 %

des victimes ont payé une rançon.

Mais **seulement** 38 %

ont pu récupérer des données et services non corrompus.

71 %

ont fait l'objet d'une **nouvelle compromission.**

63 %

ont été à nouveau compromises **dans les six mois.**

53 %

de ces entreprises ont reçu une **demande de rançon supérieure** lors de la deuxième attaque.

19 %

ont été compromises par le même groupe cyber.

52 %

ont été compromises par un autre attaquant.

Une note salée

Les entreprises françaises versent la rançon moyenne la plus élevée parmi les organisations sondées. Mais si l'on considère le coût réel d'une attaque, **cette rançon n'est que la partie émergée de l'iceberg.**

$1 million

La rançon moyenne payée par les entreprises françaises au cours des 24 derniers mois s'élève à.

Le coût réel est bien **supérieur.**

Il inclut :

- La fermeture temporaire
- L'atteinte à l'image de marque
- La perte de revenus
- Les démissions de dirigeants
- Des licenciements

50 %

accusent une **perte totale estimée entre 1 et 10 millions $.**

11 %

accusent une **perte totale estimée à plus de 10 millions $.**

94 %

des entreprises françaises **ont souscrit à une assurance Cyber.**

Mais **seulement** 25 % **ont la certitude que ces polices couvrent les attaques par ransomware.**

Seules 47 % des organisations ayant rempli une déclaration de sinistre **ont été indemnisées en totalité.**

Il est difficile de mettre en place les équipes et les plans nécessaires

La plupart des entreprises françaises ont augmenté leurs investissements en cybersécurité à la suite d'une compromission, mais les risques subsistent.

Seulement un tiers des organisations **estiment être préparées à affronter une nouvelle attaque.**

76 %

ont augmenté leurs dépenses.

Pourtant, **seulement** 32 % pensent avoir **mis en place les équipes et les plans nécessaires** pour gérer la prochaine offensive.

Ils investissent dans :

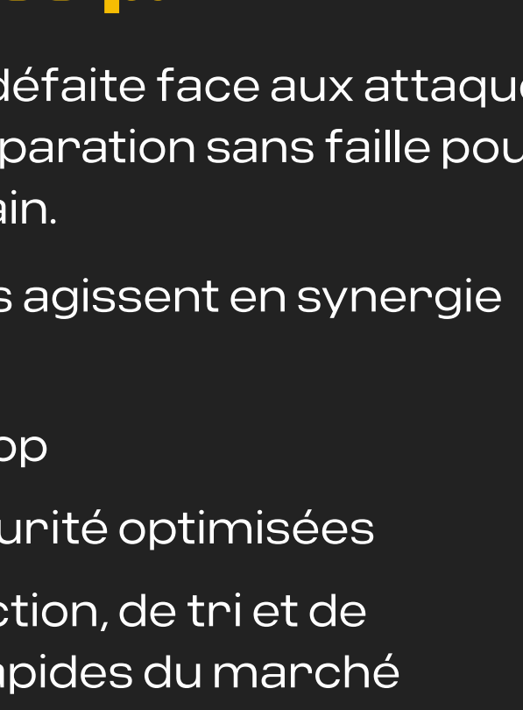
- Les talents en cybersécurité
- Les formations de sensibilisation
- Les portefeuilles de cryptomonnaies
- Les nouvelles technologies (p. ex. protection des terminaux et gestion des identités)
- La mise en conformité interne et de la supply chain
- Des contrats de cyberassurance

34 %

ont les bonnes équipes mais pas le bon plan.

30 %

ont le bon plan mais pas les bonnes équipes.



Ne cédez pas au chantage

Verser des millions de dollars aux gangs de ransomware n'est pas toujours la bonne solution.

Cela ne constitue en rien une garantie contre :

- La récupération de systèmes et données corrompus
- La revente de vos données sur le dark web
- Une nouvelle attaque

D'ailleurs, il est fort probable que votre entreprise soit à nouveau compromise.

Pour rendre votre entreprise invincible, misez sur une protection pilotée par l'IA

Cybereason, c'est zéro défaite face aux attaques d'aujourd'hui. Et une préparation sans faille pour affronter celles de demain.

Nos solutions et services agissent en synergie pour vous offrir :

- Une protection non-stop
- Des opérations de sécurité optimisées
- Les capacités de détection, de tri et de remédiation les plus rapides du marché

Lisez l'étude complète

Nous avons interrogé plus de 1 000 professionnels de cybersécurité dont l'entreprise a été victime d'un ransomware au moins une fois au cours des 24 derniers mois.

Les résultats ont de quoi surprendre.

Lire le rapport complet

Aux côtés des équipes SSI, l'entreprise de XDR Cybereason neutralise les attaques sur les terminaux, dans le cloud et dans l'ensemble de l'écosystème d'entreprise. Face aux ransomwares de dernière génération et aux techniques d'attaques sophistiquées, seule la plateforme Cybereason Defense pilotée par IA assure une protection redoutable grâce à ses fonctions de prévention, détection et réponse prédictives. En cas d'attaque, Cybereason MalOpTM délivre instantanément des données contextualisées d'une précision incomparable pour chaque appareil, utilisateur et système touché. Avec Cybereason, les informations CTI deviennent des éclairages actionnables, pour des décisions avisées au rythme de l'activité. Basée à La Jolla en Californie et forte d'une base client couvrant plus de 40 pays, Cybereason est une entreprise internationale à capitaux privés.

cybereason