Mars 2023

ÉTUDE DE MARCHÉ

Rapport 2023 sur les ransomwares

La prévalence et l'impact des attaques par ransomware dans le monde »

Barracuda®
Your journey, secured.

Sommaire

Introduction

Ransomware: une menace persistante et en constante évolution

Un ransomware est un logiciel malveillant conçu pour infecter le réseau d'une cible afin de verrouiller les données et les systèmes jusqu'à ce qu'une rançon soit payée. Dans le cas contraire, les informations sensibles ou confidentielles des victimes peuvent être volées et rendues publiques. Il s'agit d'une menace diversifiée, en constante évolution et dont le modèle criminel est lucratif, puisque souvent disponible en tant que service et accessible aux adversaires quels que soient leurs ressources ou leur niveau de compétence.

Toutes les entreprises sont des cibles potentielles. Les attaques par ransomware peuvent paralyser les opérations quotidiennes et les chaînes logistiques des clients, provoquant ainsi le chaos et des pertes financières. La réputation de l'entreprise tout comme les relations avec ses clients peuvent en souffrir.

Dans le cadre de notre enquête internationale, nous avons interrogé plusieurs entreprises sur les attaques par ransomware dont elles ont été victimes au cours des 12 derniers mois. Les résultats montrent que près des trois quarts (73%) des personnes interrogées déclarent avoir été victimes d'au moins une attaque par ransomware en 2022 et 38% déclarent avoir été touchées deux fois ou plus.

Les entreprises ayant subi plusieurs attaques par ransomwares ont été plus nombreuses à dire qu'elles avaient payé la rançon pour récupérer les données chiffrées. Parmi celles ayant été prises pour cible une fois, 31% ont payé la rançon pour récupérer les données chiffrées contre 34% pour celles touchées deux fois et 42 % pour celles touchées trois fois ou plus. Les entreprises ayant subi plusieurs attaques étaient également moins nombreuses à utiliser un système de backup de données pour les aider à les récupérer.

Les résultats montrent que 69% des entreprises ont d'abord reçu un e-mail malveillant, tel qu'un email de phishing conçu pour voler des identifiants afin d'accéder au réseau et permettre aux cybercriminels de rechercher des actifs, des serveurs et des bases de données avant de lancer l'attaque par ransomware. Les applications web et le trafic web sont les deuxièmes moyens

préférés par les pirates et représentent une menace croissante dans la mesure où il y a toujours plus de contenu à cibler.

Les entreprises qui ont souscrit une cyber assurance étaient plus susceptibles d'être victimes des ransomwares.

En effet, plus des trois quarts (77%) des entreprises bénéficiant d'une cyber assurance ont été victimes d'au moins une attaque par ransomware, contre 65 % des entreprises n'étant pas assurées. Cela peut signifier que les cybercriminels sont plus susceptibles de cibler les entreprises assurées, convaincus que les assureurs seront prêts à couvrir le coût de la rançon pour accélérer la récupération.

Cette étude a également révélé que plus d'un quart (27%) des entreprises interrogées déclarent ne pas être totalement prêtes à faire face à une attaque par ransomware.

Le secteur de la sécurité a un rôle essentiel à jouer : il doit aider les entreprises à faire face à la menace des ransomwares grâce à des technologies de sécurité approfondies et multicouches, à la chasse aux menaces, à des capacités de détection et de réponse étendues (XDR), ainsi qu'à une réponse efficace aux incidents pour détecter les intrus et combler les lacunes afin d'empêcher les pirates de s'y introduire facilement.

Méthodologie

Barracuda a chargé le cabinet d'étude indépendant Vanson Bourne de mener une enquête mondiale auprès de responsables informatiques et de professionnels techniques du secteur, de responsables de la sécurité informatique et de décideurs de haut niveau en matière d'informatique et de sécurité informatique. Les 1 350 participants à cette enquête travaillent dans divers secteurs, notamment l'agriculture, les biotechnologies, la construction, l'énergie, le secteur public, la santé, l'industrie manufacturière, la distribution, les télécommunications, le commerce de gros et d'autres secteurs. Les participants à l'enquête travaillent aux États-Unis, en Australie, en Inde et en Europe. En Europe, les pays représentés sont : le Royaume-Uni, la France, le DACH (Allemagne, Autriche, Suisse), le Benelux (Belgique, Pays-Bas, Luxembourg) et les pays nordiques (Danemark, Finlande, Norvège, Suède). L'enquête a été soumise en décembre 2022.

Le rapport fait également référence aux recherches commandées par Barracuda publiées en 2019. L'enquête comprenait les réponses de 660 cadres, contributeurs individuels et chefs d'équipe exerçant des fonctions liées à la sécurité informatique en Amérique, ainsi que dans les zones de l'EMEA et de l'APAC.

CONSTAT N° 1

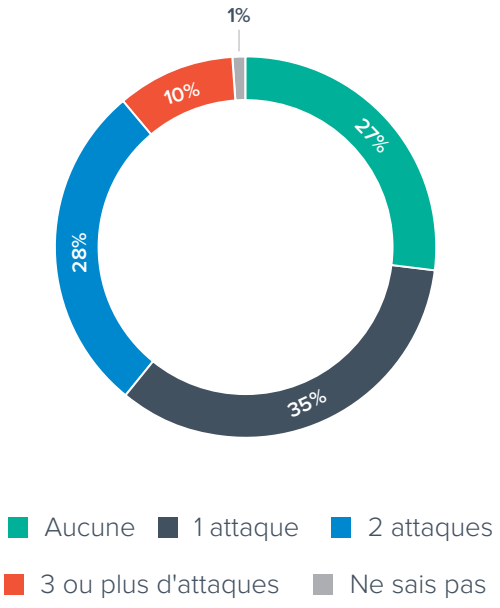
La plupart des entreprises ont été la cible d'une attaque par ransomware et un tiers en ont subi deux fois ou plus

Près de trois quarts des entreprises interrogées (73%) ont signalé avoir été victimes d'au moins une attaque par ransomware au cours des 12 derniers mois.

La proportion élevée d'entreprises victimes des ransomwares n'a rien de surprenant. En effet, les hackers se tournent de plus en plus vers le modèle RaaS (Ransomware-as-a-service), ce qui permet aux pirates de lancer plus facilement, et à moindres coûts, des attaques par ransomware, souvent avec peu voire aucune connaissance technique nécessaire. Le RaaS est un malware payant dans le cadre duquel les développeurs louent leur infrastructure de ransomware à d'autres cybercriminels.

Combien d'attaques par ransomware votre entreprise a-t-elle subies au cours des 12 derniers mois ?

(n=1,350)



Plus d'un tiers (38%) des entreprises interrogées ont déclaré avoir été victimes d'au moins deux attaques par ransomware au cours des 12 derniers mois.

Le fait que plusieurs attaques réussissent suggère que les failles de sécurité ne sont pas entièrement traitées après le premier incident.

Cela peut s'expliquer de plusieurs raisons. Par exemple, un manque de contrôles de sécurité, de capacités de réponse aux incidents et d'investigation, ajouté aux techniques toujours plus sophistiquées et furtives des pirates, pourrait indiquer que les portes dérobées implantées ou les autres outils de persistance laissés par les pirates ne sont pas identifiés et supprimés. Il se peut que les points d'accès soient laissés ouverts et que les mots de passe du compte ne soient pas réinitialisés de sorte que les identifiants volés puissent être utilisés à nouveau.

La neutralisation complète d'une attaque est d'autant plus difficile, car les pirates détournent souvent des outils d'administration informatique légitimes qui sont également utilisés par les équipes informatiques à des fins professionnelles banales et quotidiennes. Ainsi, leur apparence sur le réseau ne peut pas éveiller immédiatement les soupçons.

Différence selon les secteurs

Les secteurs d'activité ciblés par les ransomwares varient considérablement. Par exemple, la quasi-totalité (98%) des entreprises de services aux consommateurs a subi au moins une attaque par ransomware.

Les services aux consommateurs traitent souvent un grand nombre de données personnelles sur les clients et reçoivent une quantité importante de communications provenant de l'extérieur de leur entreprise, ce qui en fait une bonne cible pour les ransomwares. Dans le même temps, seulement 22% des personnes interrogées dans ce secteur ne se sentaient pas suffisamment prêtes à faire face à une attaque par ransomware.

Les entreprises du secteur de l'énergie, du pétrole/gaz et des services publics ont également signalé un taux de réussite des attaques par ransomware supérieur à la moyenne (85%). Les infrastructures critiques deviennent des cibles populaires, compte tenu de l'ampleur des perturbations que les attaques par ransomware peuvent causer et l'importance des gains potentiels.

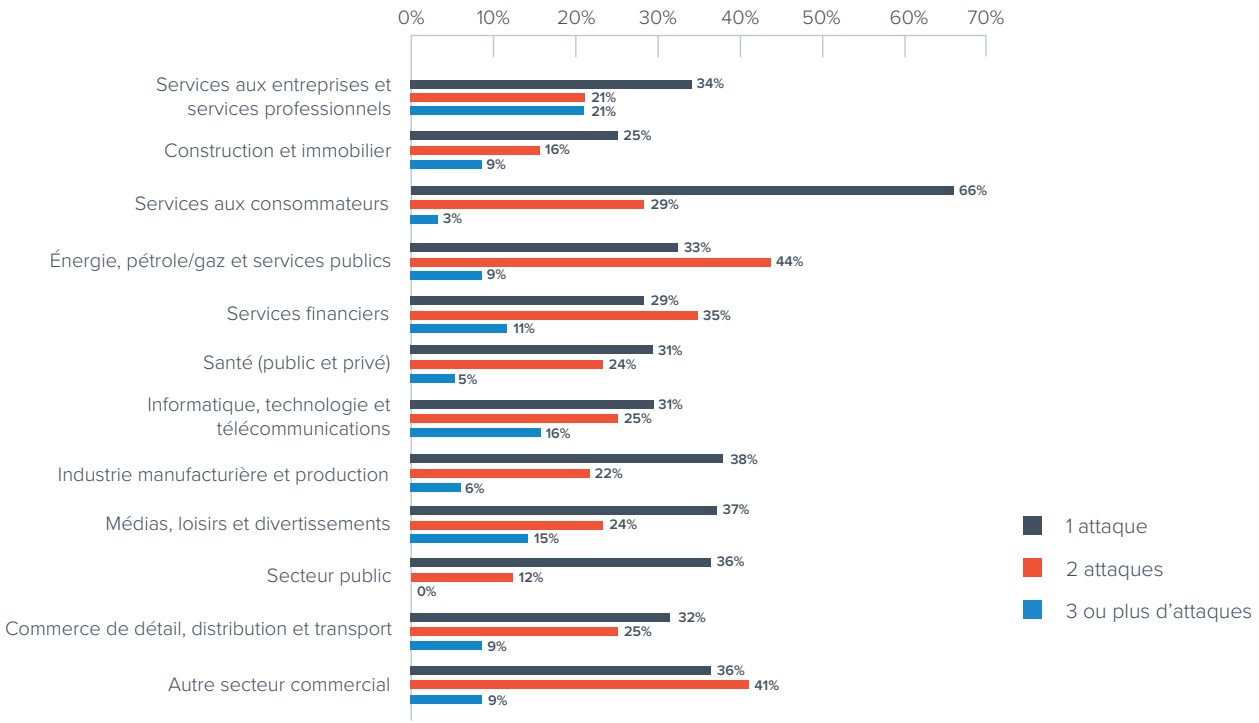
Notre étude de l'année dernière sur les attaques par ransomware signalées publiquement a montré que le nombre d'attaques liées à l'infrastructure a été multiplié par quatre, ce qui montre que les cybercriminels ne cherchent aujourd'hui plus à toucher uniquement la première victime, mais à causer des dommages dans un rayon beaucoup plus vaste.

Les entreprises du secteur de l'énergie, du pétrole/gaz et des services publics sont également les plus susceptibles de subir plusieurs attaques, 53% d'entre elles ayant signalé au moins deux incidents de ransomware, contre 38 % pour l'ensemble des entreprises.

46 % des entreprises des services financiers ont déclaré avoir été ciblées deux fois ou plus. Les cibles de premier plan des ransomwares, telles que le secteur de la santé, étaient moins susceptibles d'être victimes d'attaques multiples, seulement 29% des personnes interrogées dans ce secteur ayant déclaré avoir été ciblées par au moins deux attaques.

Nombre d'attaques par ransomware en 12 mois par secteur

(n=1,350)



CONSTAT N° 2

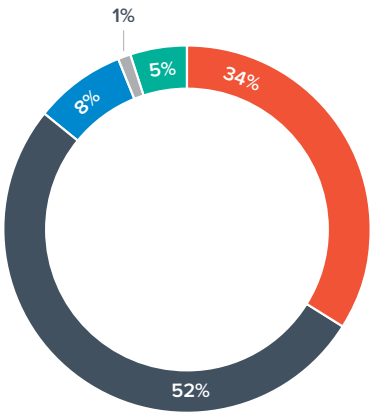
Les victimes ayant subi plusieurs attaques sont plus enclines à payer la rançon pour récupérer les données chiffrées

Une attaque par ransomware réussie chiffre généralement des données précieuses au sein d'une entreprise. 95% des entreprises interrogées qui ont subi une attaque par ransomware au cours des 12 derniers mois ont déclaré que leurs données étaient chiffrées, ce qui a considérablement perturbé leurs activités.

Dans l'ensemble, seulement 1% ont perdu les données chiffrées, 34% ont choisi de payer la rançon et 52% ont utilisé leurs systèmes de backup pour récupérer les données.

Les cybercriminels ont-ils réussi à chiffrer les données de votre entreprise lors de la plus importante attaque par ransomware des 12 derniers mois?

(n=982)



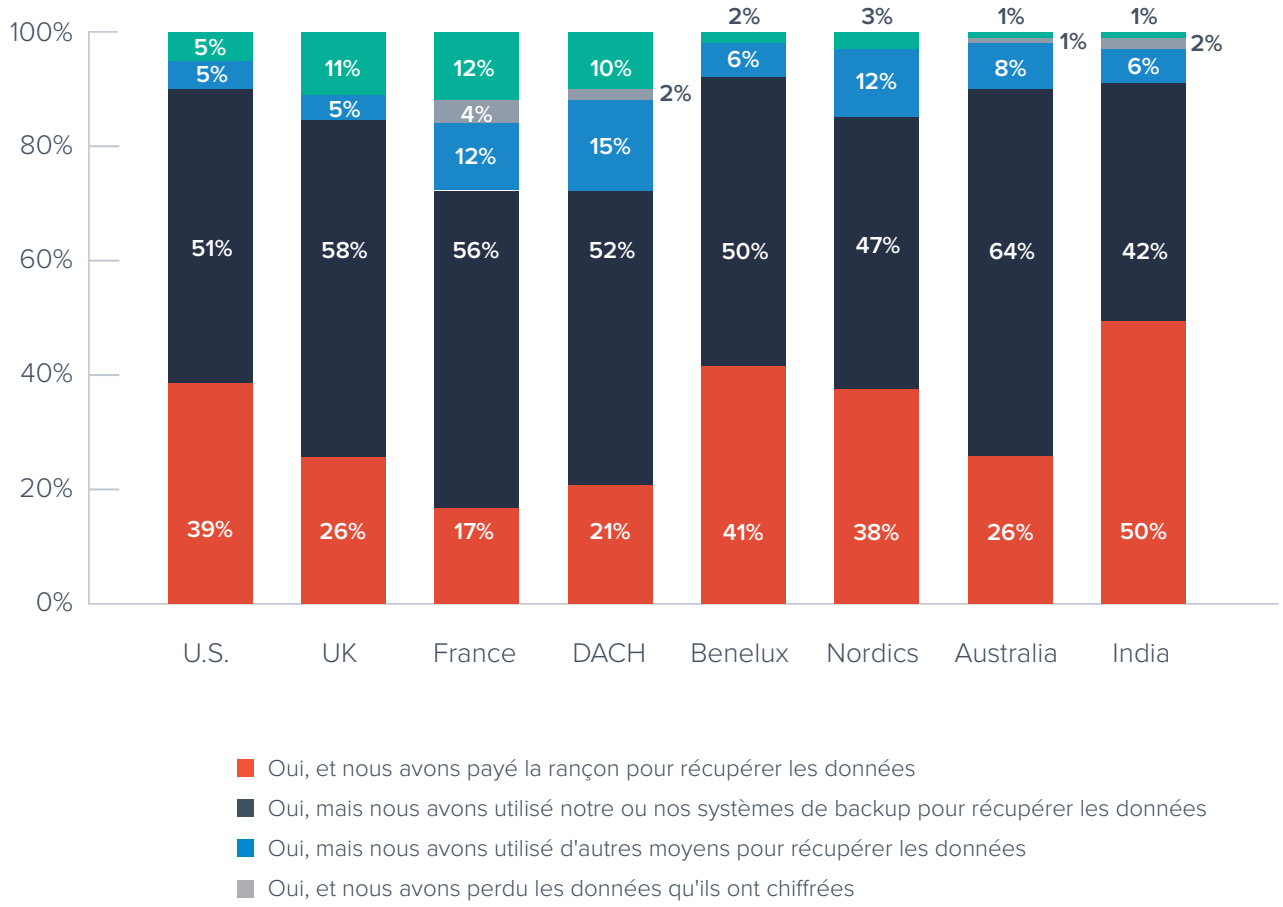
- Oui, et nous avons payé la rançon pour récupérer les données
- Oui, mais nous avons utilisé notre ou nos systèmes de backup pour récupérer les données
- Oui, mais nous avons utilisé d'autres moyens pour récupérer les données
- Oui, et nous avons perdu les données qu'ils ont chiffrées
- Non, ils n'ont pas chiffré les données

La proportion à céder au chantage, quel que soit le nombre d'attaques, variait considérablement selon le pays et le secteur.

Les entreprises du Royaume-Uni, de la France, des pays du DACH et de l'Australie étaient moins nombreuses à payer la rançon pour récupérer leurs données, tandis qu'en Inde, la rançon a été payée une fois sur deux. Dans la quasi-totalité des pays, les entreprises récupéraient leurs données à partir d'une sauvegarde.

Les cybercriminels ont-ils réussi à chiffrer les données de votre entreprise lors de la plus importante attaque par ransomware des 12 derniers mois?

(n=982)

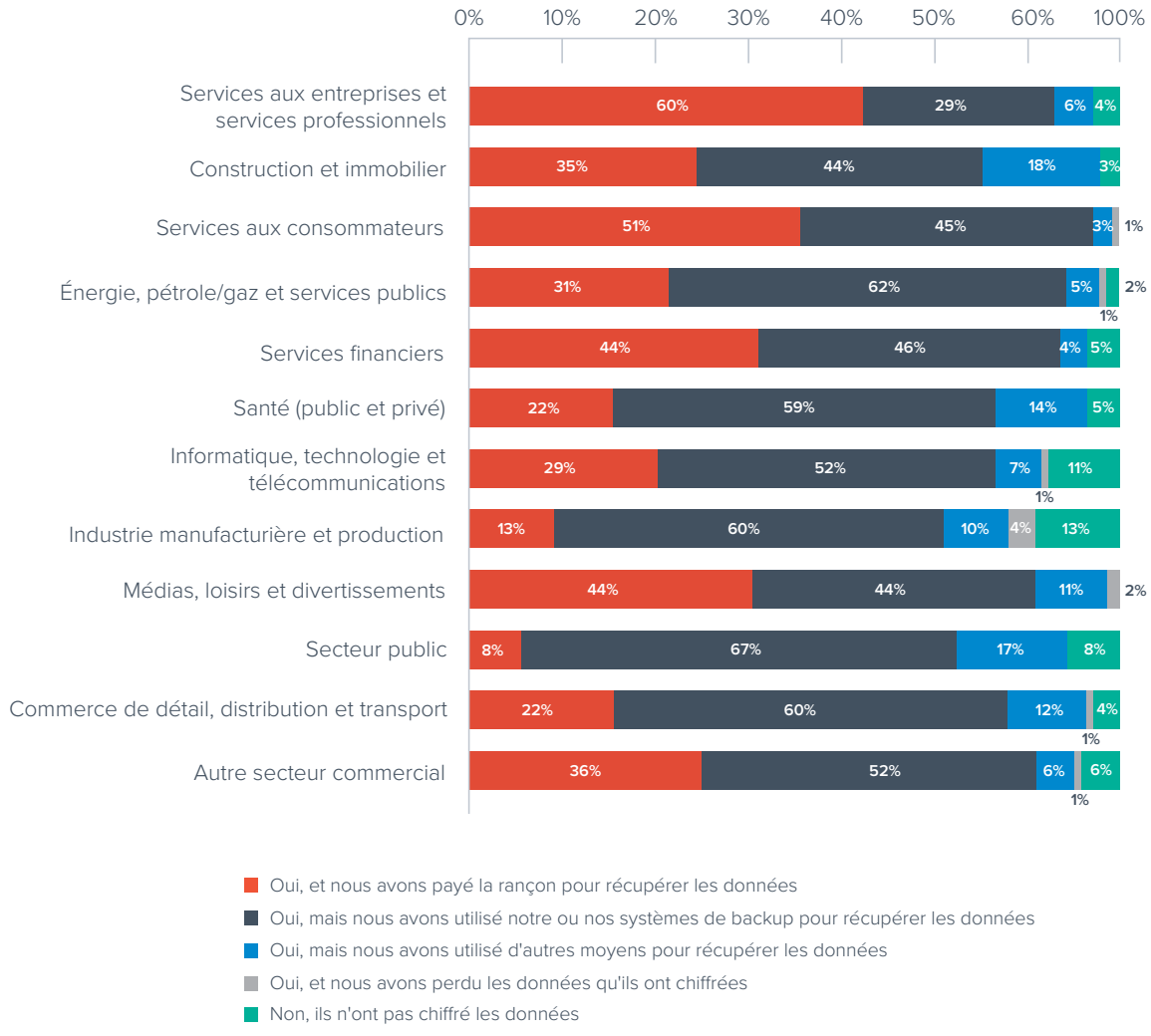


Les entreprises du secteur des services aux entreprises et services professionnels étaient les plus enclines à payer la rançon pour récupérer les données : 60% d'entre elles ont payé. Les organisations de services aux consommateurs ont payé la rançon dans 51 % des cas, tandis que les organisations de services financiers et de médias, de loisirs et de divertissement ont payé dans 44% des attaques.

Les établissements de santé étaient moins enclins à payer la rançon et ne l'ont fait que dans 22% des cas.

Les cybercriminels ont-ils réussi à chiffrer les données de votre entreprise lors de la plus importante attaque par ransomware des 12 derniers mois?

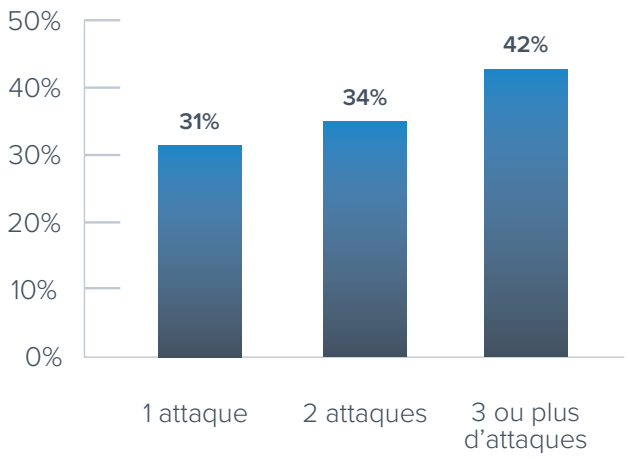
(n=982)



L'enquête a révélé que les entreprises les plus souvent touchées par des ransomwares étaient également plus enclines à payer la rançon pour restaurer des données chiffrées : 42% des entreprises ayant subi trois attaques ou plus ont payé la rançon. Elles étaient également moins susceptibles d'utiliser un système de backup des données pour les aider à récupérer leurs données.

Entreprises qui ont payé la rançon pour restaurer des données chiffrées

(n=982)



D'autres enquêtes confirment que la proportion d'entreprises qui ont payé la rançon malgré ou peut-être du fait d'avoir été victime d'au moins deux attaques par ransomware. Par exemple, une étude réalisée en 2022 sur le paiement de rançons a révélé que 80 % des victimes de ransomware qui paient la rançon sont touchées une deuxième fois et paient souvent à nouveau la rançon.

L'une des explications possibles du lien entre les attaques multiples et les paiements par ransomware est qu'une fois que l'on sait qu'une entreprise est prête à payer, d'autres pirates s'en prennent à la même victime.

Les marchés clandestins et les courtiers d'accès initiaux (IAB) sont susceptibles d'accorder une grande importance aux identifiants d'accès aux victimes dont on sait qu'elles sont prêtes à payer et à rester vulnérables. Dans certains cas, les mêmes pirates reviennent pour en obtenir davantage.

Investir dans une solution de protection des données qui permet de sauvegarder et de restaurer des données peut aider à éviter de payer une rançon qui pourrait autrement encourager les cybercriminels à attaquer à nouveau.

CONSTAT N° 3

L'e-mail est le point de départ le plus courant d'attaque par ransomware

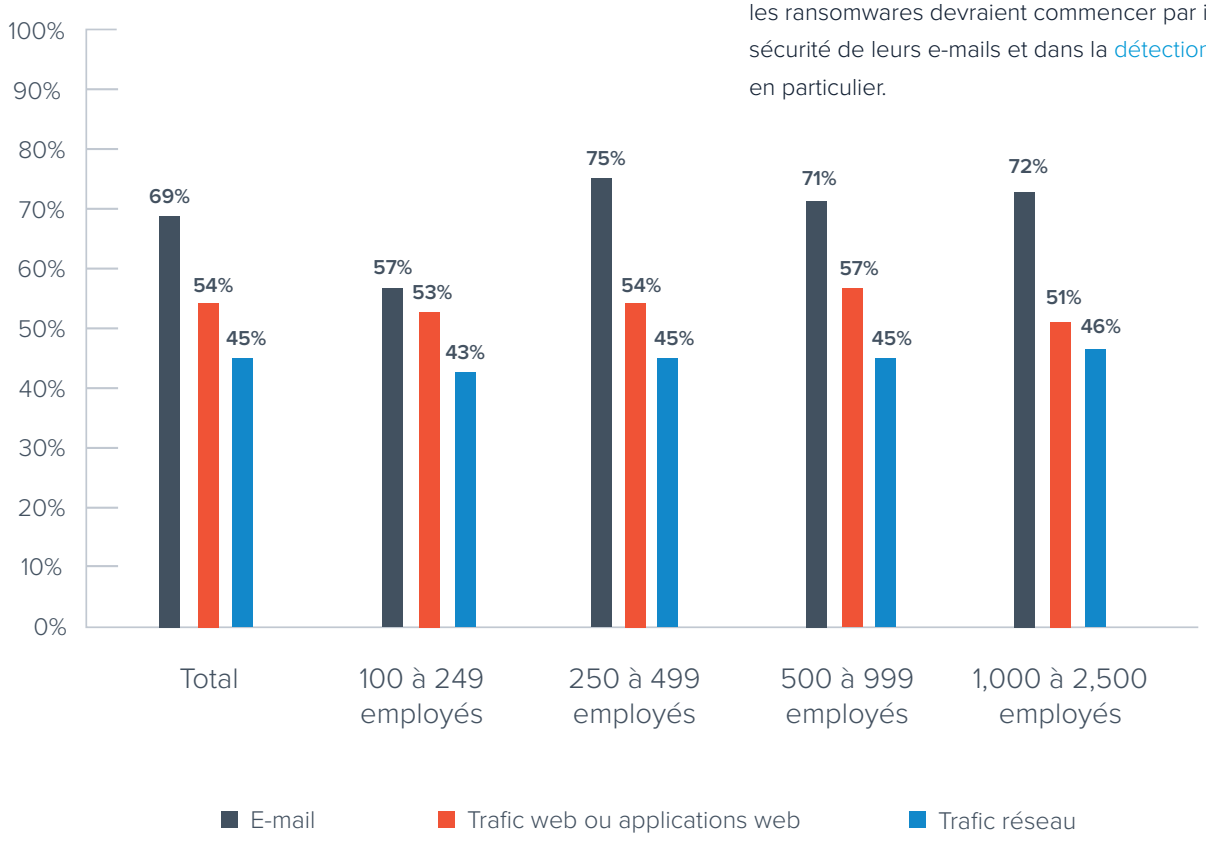
69% des entreprises ont d'abord reçu un e-mail malicieux.

Ce pourcentage est supérieur à la moyenne (75%) pour les entreprises légèrement plus grandes avec plus de 250 employés. Il est beaucoup plus simple d'envoyer un e-mail que de pénétrer dans le réseau d'une entreprise.

Traditionnellement, les hackers joignaient un document avec une charge utile malveillante ou une URL menant à un faux site web capable de distribuer des malwares. Au fur et à mesure, les entreprises ont déployé une protection avancée contre les menaces telle que le sandboxing et la protection URL au moment du clic. Les cybercriminels se sont alors tournés vers des tactiques de social engineering pour hameçonner les identifiants de connexion des utilisateurs. Les comptes compromis peuvent être une rampe de lancement facile pour les attaques par ransomware, permettant aux cybercriminels de se déplacer latéralement au sein de l'entreprise et d'éviter d'être détectés. Les entreprises qui souhaitent améliorer leurs défenses contre les ransomwares devraient commencer par investir dans la sécurité de leurs e-mails et dans la détection dédiée du phishing en particulier.

D'où proviennent les attaques par ransomware subies par votre entreprise?

(n=982)

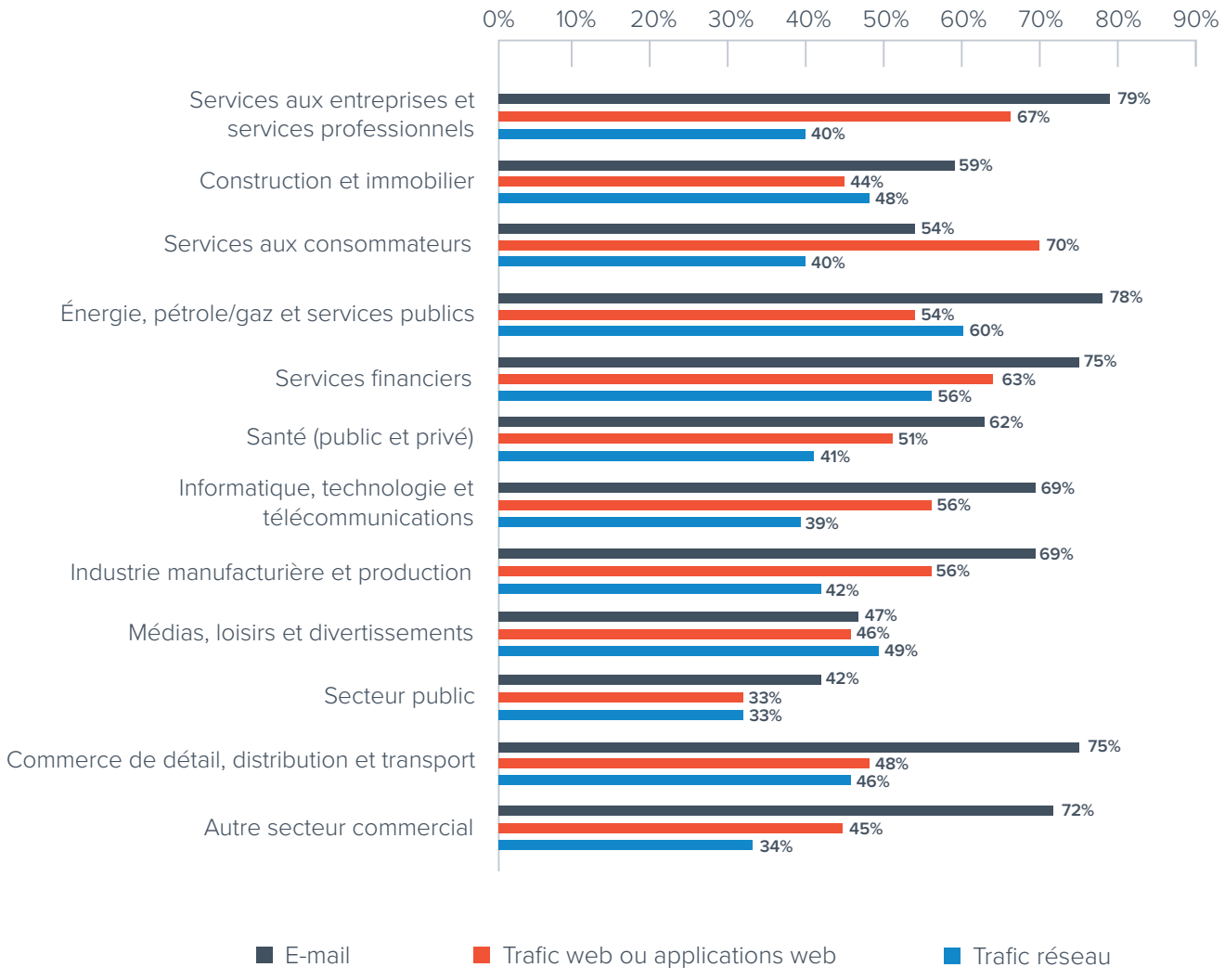


Cependant, l'e-mail n'est pas le premier vecteur de menace des ransomwares pour tous les secteurs. Par exemple, la plupart des attaques par ransomware dans les services grand public proviennent du trafic web et des applications web.

Les applications en ligne telles que les services de partage de fichiers, les formulaires web et les sites de commerce électronique peuvent être compromis par des pirates. Les applications web sont attaquées par le biais de l'interface utilisateur ou d'une interface API. Souvent, ces attaques impliquent le credential stuffing, des attaques par force brute ou des vulnérabilités OWASP. Une fois l'application compromise, le pirate peut introduire un ransomware et d'autres malwares dans le système. Ceux-ci peuvent ensuite infecter le réseau ainsi que les utilisateurs de l'application.

D'où proviennent les attaques par ransomware subies par votre entreprise?

(n=982)



CONSTAT N° 4

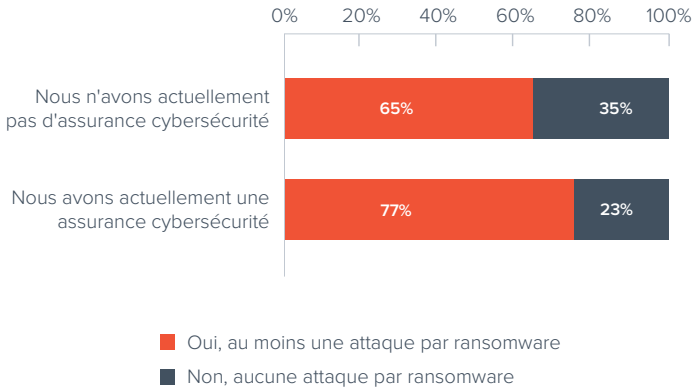
Les entreprises qui ont souscrit une cyber assurance sont plus susceptibles d'être victimes de ransomwares

63% des entreprises interrogées ont investi dans une assurance cybersécurité pour les aider à minimiser les coûts associés à toute violation de données. Bien que les entreprises de cyber assurance puissent aider à négocier les paiements de rançon ou même à fournir les fonds pour le paiement, les entreprises sont souvent confrontées à une facture très élevée en raison des nombreuses exclusions prévues par leurs polices d'assurance.

Les entreprises qui ont souscrit une cyber assurance étaient plus susceptibles d'être victimes d'une attaque par ransomware au cours de l'année écoulée. **77% d'entre elles ont été victimes d'une attaque par ransomware, contre 65% sans cyber assurance**. Cela peut signifier que les cybercriminels sont plus susceptibles de cibler les entreprises assurées, convaincus que les assureurs seront prêts à couvrir le coût de la rançon pour accélérer la récupération.

Votre entreprise a-t-elle subi au moins une attaque par ransomware au cours des 12 derniers mois?

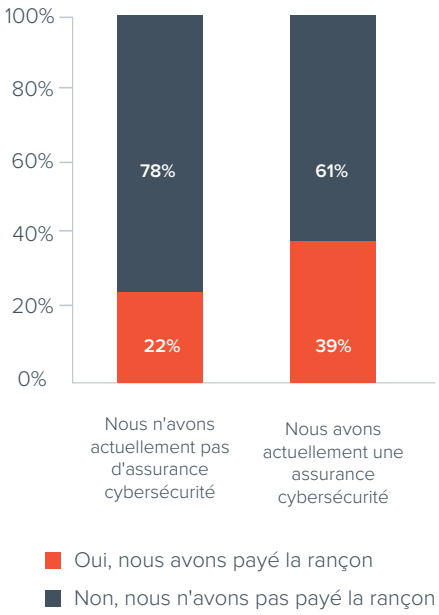
(n=1,350)



Par exemple, les résultats de l'enquête montrent que **les entreprises ayant souscrit une cyber assurance étaient plus enclines à payer la rançon pour récupérer leurs données (39% contre 22% des organisations sans cyber assurance**). Bien qu'il soit impossible d'établir une connexion, il convient également de noter que **les entreprises ciblées par au moins deux attaques par ransomware étaient également plus susceptibles de souscrire une cyber assurance (70%).**

Avez-vous payé la rançon pour récupérer les données?

(n=982)



CONSTAT N° 5

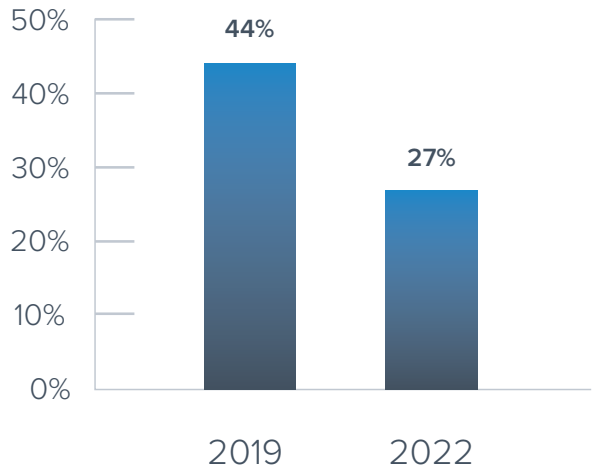
De nombreuses entreprises estiment ne pas être totalement prêtes à faire face aux ransomwares

Plus d'un quart (27%) des entreprises interrogées déclarent ne pas être totalement prêtes à faire face à une attaque par ransomware.

Il s'agit d'une amélioration d'une étude antérieure menée en 2019, alors que près de la moitié (44%) ont déclaré ne pas être prêtes à faire face à une attaque par ransomware. Depuis 2019, nous avons assisté à des attaques par ransomware très médiatisées qui ont entraîné des pertes financières importantes. La vaste publicité faite autour de ces attaques a probablement incité de nombreuses entreprises à investir dans leur sécurité et à se préparer à d'éventuelles attaques par ransomware.

L'UE n'est pas totalement prête à faire face aux ransomwares

(n=660 pour 2019 ; n=1 350 pour 2022)

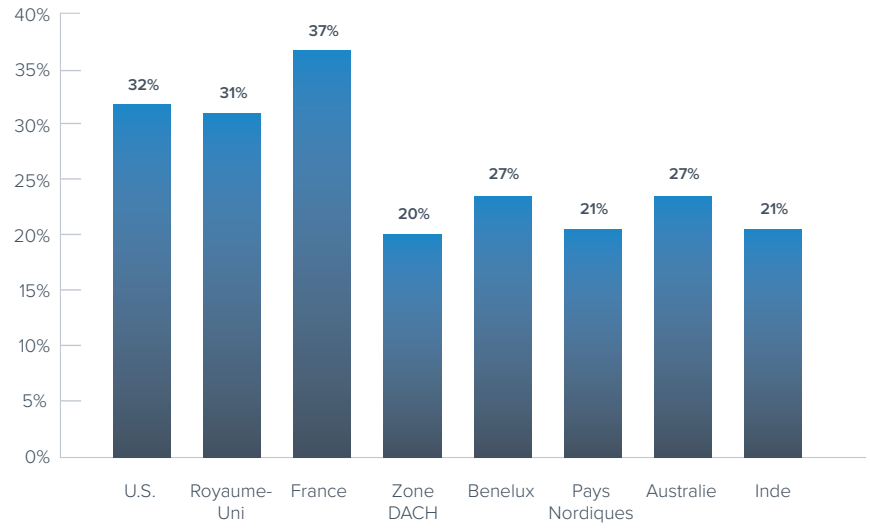


De précédentes recherches de NordLocker ont révélé que les États-Unis, le Royaume-Uni, le Canada et la France connaissent le plus grand nombre d'attaques par ransomware au niveau mondial. Notre étude a également mis en évidence que les participants des États-Unis, du Royaume-Uni et de la France s'estiment moins prêts à faire face aux ransomwares.

Dans la plupart des cas, le nombre d'attaques leur semble accablant et ils craignent que le nombre élevé n'augmente les chances de succès des acteurs de la menace. Les grandes entreprises s'estiment également moins prêtes, car elles disposent d'un grand volume de données à protéger et d'une surface d'attaque beaucoup plus importante.

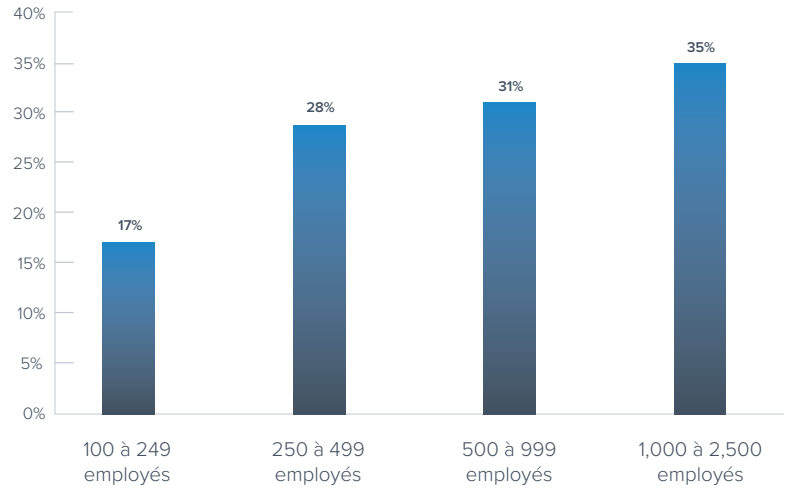
L'UE n'est pas totalement prête à faire face aux ransomwares

(n=1,350)



L'UE n'est pas totalement prête à faire face aux ransomwares

(n=1,350)



Vous trouverez de plus amples informations et des conseils pratiques sur la façon de vous protéger contre les ransomwares dans le document Ne payez pas la rançon : un guide en trois étapes pour se protéger contre les ransomwares, qui comprend une liste de contrôle téléchargeable pour vous lancer.

Conclusion

Les entreprises ont besoin d'une sécurité intégrée et multicouche pour protéger leur surface d'attaque toujours plus grande contre les menaces en constante évolution telles que les ransomwares. Voici les principaux domaines de cybersécurité sur lesquels vous devez vous concentrer pour minimiser vos risques et votre exposition aux ransomwares et autres cybermenaces.

- **Protégez vos identifiants.** La protection des identifiants nécessite une approche en deux phases : investir d'abord dans des outils de détection et de réponse, puis vous concentrer sur la formation de vos utilisateurs.

- La technologie de protection des e-mails doit être en mesure de détecter les charges utiles malveillantes transmises par des liens ou dans des pièces jointes et de reconnaître les attaques faisant appel à des tactiques de social engineering avancées conçues pour contourner les technologies de filtrage et inciter les utilisateurs à agir. Votre solution de sécurité des e-mails doit intégrer la technologie d'apprentissage machine, car elle identifiera les attaques de social engineering avec plus de précision. Pour cela, elle recherche la moindre variante d'une forme de communication habituelle.

- Il est également important que les employés sachent reconnaître et signaler les e-mails suspects. Utilisez des outils tels que la simulation de phishing, et testez l'efficacité d'une formation.

- **Accès sécurisé aux comptes, aux applications et aux réseaux.** L'authentification multifactorielle (MFA) reste une best practice qui devrait être adoptée par toutes les entreprises. Cependant, les pirates ont trouvé des moyens de la contourner. Envisagez de mettre en place une stratégie d'accès Zero Trust plus avancée qui vérifie en permanence les utilisateurs et les appareils et autorise uniquement les utilisateurs autorisés à accéder aux bonnes ressources.

- **Sécurisez vos applications web.** Les applications en ligne telles que les services de partage de fichiers, les formulaires web ou encore les sites d'e-commerce peuvent être compromis par des pirates informatiques. Les applications sont souvent ciblées via l'interface utilisateur ou une interface API. Envisagez de mettre en place une sécurité applicative basée sur les API et un web application firewall qui assurera une sécurité multicouche pour bloquer les menaces avancées, notamment les attaques zero-day, la prévention des intrusions et le sandboxing des malwares ainsi que la segmentation avancée du réseau pour empêcher les mouvements latéraux.

- **Sauvegardez vos données.** Pour protéger votre entreprise de l'impact total d'une attaque par ransomware, les données doivent être correctement sauvegardées et isolées en toute sécurité, même lorsqu'elles se trouvent dans le cloud. Vous devez également vous assurer que le backup de vos données vous permettra de restaurer les données dans un délai raisonnable, alors testez régulièrement votre processus de récupération de backup pour vérifier son fonctionnement.

- **Développez une défense approfondie grâce à des informations sur les menaces, au processus de réponse aux incidents et à la technologie XDR.** Le lancement du ransomware est souvent la dernière étape de l'attaque et peut être précédé, par exemple, par un mouvement latéral, une exfiltration de données, une installation d'outils supplémentaires, etc. Si vous parvenez à détecter et à bloquer l'attaque à ces stades précoces, vous pourriez être en mesure d'empêcher l'impact total du ransomware.

- C'est là qu'interviennent des services tels que XDR (extended detection and response), qui offre une visibilité sur l'ensemble d'un environnement informatique, étayé par des informations sur les menaces mises à jour en permanence. XDR et d'autres solutions de réponse aux incidents vous aideront à identifier, contenir et neutraliser les incidents avant qu'ils ne s'aggravent.

- Il est également important de rester informé de l'évolution du champ des menaces, y compris des comportements et des outils les plus récents des pirates, afin de savoir à quoi s'attendre et comment réagir. Vous devez vous efforcer d'enquêter sur tout ce qui ne semble pas correct. Si vous craignez de ne pas avoir les ressources nécessaires pour le faire, envisagez de recourir aux services d'un centre de sécurité (SOC) externe, par exemple, dans le cadre de votre plateforme XDR, qui surveillera votre réseau en continu et enquêtera sur les comportements anormaux ou suspects.

A propos de Barracuda

Rendre le monde plus sûr est notre objectif chez Barracuda. Nous pensons que chaque entreprise doit se doter de solutions cloud-first, faciles à acquérir, à déployer et à utiliser, tout en gardant leur niveau de sécurité. Nous protégeons les e-mails, les réseaux, les données et les applications avec des solutions innovantes et évolutives, qui s'adaptent à la croissance de nos clients. Plus de 220 000 entreprises à travers le monde font confiance à Barracuda pour les protéger – elles restent sereines face aux risques qui sont toujours là – et peuvent se concentrer sur le développement de leur business.

Pour plus d'informations, visitez le site barracuda.com.

A propos de Vanson Bourne

Vanson Bourne est un cabinet indépendant spécialiste des études de marché pour le secteur des technologies. Leur réputation de produire des analyses solides, fiables et basées sur des études est elle-même fondée sur des principes rigoureux ainsi que sur leur capacité à interroger des décisionnaires majeurs qui occupent des fonctions techniques et métier dans tous les secteurs et sur les marchés principaux.

Pour en savoir plus, accédez à vansonbourne.com.

Barracuda®
Your journey, secured.