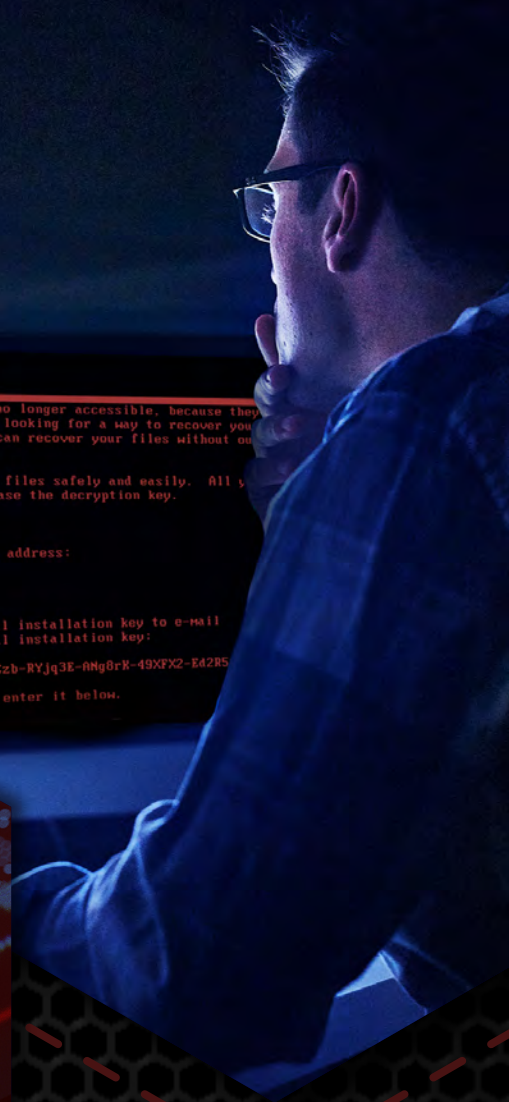




Rapport 2021 sur l'impact des ransomwares

Sommaire

- 3 Introduction et méthodologie
- 4 Les conséquences d'une formation insuffisante à la cybersécurité
- 5 Payer ou ne pas payer ?
- 6 Les coûts indirects élevés des ransomwares
- 7 Les chiffres des attaques ne sont pas communiqués
- 15 À propos de Keeper

Introduction et méthodologie

2021 est l'année des ransomwares. Alors que la fréquence des attaques augmente de manière fulgurante, de vertigineuses demandes de rançons font la une des médias. Jusqu'à présent relativement épargnés par les répercussions de ces attaques, les consommateurs sont désormais confrontés aux pénuries de produits et à la difficulté d'accéder aux services lorsque les entreprises sont victimes des ransomwares.

Mais après une attaque, que se passe-t-il au sein de l'organisation ? Comment les processus internes sont-ils affectés ? Quel est l'impact sur l'efficacité et la productivité du personnel ? Pour le savoir, Keeper a réalisé une enquête aux États-Unis portant sur 2 000 collaboratrices et collaborateurs dont l'entreprise avait été victime d'une attaque par ransomware au cours des 12 mois précédents.

Keeper Security a confié à Pollfish la conduite de cette étude portant sur 2 000 employés aux États-Unis. Seules les personnes travaillant à plein temps au sein d'une entreprise victime d'attaque par ransomware au cours des 12 derniers mois étaient incluses dans le sondage. L'enquête a été achevée en juin 2021.

Les conséquences d'une **formation** **insuffisante à la** **cybersécurité**



Près d'un tiers des collaboratrices et collaborateurs ne disposaient pas d'une formation à la cybersécurité suffisante avant l'attaque.

La sensibilisation du personnel à la cybersécurité est essentielle afin de prévenir les attaques par ransomware, en particulier parce qu'un grand nombre d'entre elles relèvent du piratage psychologique :

- Selon les personnes interrogées, les e-mails de phishing ont entraîné 42 % des attaques par ransomware
- Les sites Internet malveillants étaient impliqués dans 23 % des attaques
- Des mots de passe compromis en ont causé 21 %

Or, 29 % des personnes interrogées ont indiqué à Keeper qu'elles ne savaient pas ce qu'était un ransomware avant que leur employeur n'en soit victime. On peut donc en déduire qu'un grand nombre voire la majorité des attaques par ransomware pourraient être évitées :

- en formant correctement et régulièrement les employés à la cybersécurité, et en particulier à la manière d'éviter le phishing et autres stratégies de piratage psychologique
- en exigeant que le personnel utilise des mots de passe forts et uniques pour tous leurs comptes, et en instaurant l'authentification multi-facteurs partout où cela est possible



BIEN, MAIS TROP TARD ?

Les personnes interrogées nous ont indiqué qu'après l'attaque, 87 % des organisations ont mis en œuvre des protocoles de sécurité plus stricts, 90 % ont dispensé à leur personnel une formation supplémentaire à la cybersécurité, et 67 % ont augmenté leurs dépenses en matière de cybersécurité.



Payer ou ne pas payer ?

Tout le monde s'accorde à dire que payer une rançon encourage de futures attaques. Cependant, la question de savoir si les entreprises doivent ou non céder aux exigences des ransomwares reste un vaste débat qui n'épargne pas les professionnels de la cybersécurité. Ces tergiversations s'expliquent par la pression phénoménale subie par les dirigeants d'une organisation attaquée : clients, parties prenantes de l'entreprise et même cyber-assureurs les pressent pour rétablir la situation et revenir en ligne le plus rapidement possible. À noter que la pression est particulièrement intense au sein des établissements de santé et dans le secteur public, où les pannes de système peuvent mettre en péril la vie et la santé des personnes.

Par conséquent, 49 % des personnes interrogées ont affirmé à Keeper que leur entreprise avait payé la rançon. Cependant, il a bien fallu trouver cet argent quelque part : 93 % des personnes interrogées ont indiqué que leur employeur avait réduit le budget d'autres postes suite au paiement de la rançon.

Les coûts indirects élevés des ransomwares

La récupération post-attaque entraîne des coûts indirects élevés.

Si les réseaux sociaux relatent surtout les demandes de rançon stratosphériques des cyber-malfaiteurs, les organisations doivent également assumer de nombreux coûts indirects après une attaque, en particulier en lien avec les arrêts de systèmes. En plus de frustrer les clients et les partenaires, ces pannes empêchent les employés de faire leur travail.

- 77 % des personnes interrogées étaient temporairement dans l'incapacité d'accéder aux systèmes ou réseaux après l'attaque
- 28 % des pannes ont duré une semaine ou plus
- 26 % des personnes interrogées n'ont pas été en mesure de mener à bien l'intégralité de leurs tâches pendant au moins une semaine

Mais une fois les systèmes rétablis, les dépenses ne s'arrêtent pas là : les organisations doivent procéder à des changements pour empêcher de nouvelles attaques. La vaste majorité des personnes interrogées (83 %) a déclaré que leur organisation a installé de nouveaux logiciels ou a réalisé d'autres mises à jour majeures, comme migrer certains actifs dans le cloud.

Dans la plupart des cas, la mise en œuvre de ces changements a impacté encore un peu plus la productivité et est venue s'ajouter aux coûts indirects de récupération ; 71 % des personnes interrogées ont déclaré que le processus d'installation de

nouveaux logiciels et mises à jour gênait ou altérait la productivité.

- 64 % des personnes interrogées ont perdu leurs identifiants ou documents de connexion
- 38 % ont indiqué avoir rencontré des problèmes techniques de programmation ou d'application
- 33 % ont été confrontés à une courbe d'apprentissage intensive concernant les nouveaux protocoles
- 40 % ont perdu du temps en raison des mises à jour fréquents et redémarrages fréquents de leur PC
- 43 % ont dû se reconnecter sans cesse à des programmes/comptes (au lieu de rester en session ouverte)
- 21 % ont déclaré que leurs outils et applications en ligne habituels n'étaient plus disponibles.

Or, c'est précisément lorsque les employés ont le plus besoin de l'aide du département informatique pour réinitialiser leurs mots de passe, tenter de récupérer des documents perdus et faire fonctionner les nouvelles applications et protocoles que les équipes IT sont débordées. Plus d'un tiers (36 %) des personnes interrogées ont déclaré avoir eu un accès limité au support informatique pour des problèmes indépendants de la sécurité après une attaque.

Les chiffres des attaques ne sont pas communiqués

Les attaques par ransomware sont beaucoup plus répandues qu'on ne le pense, car un grand nombre d'entre elles ne sont pas déclarées.

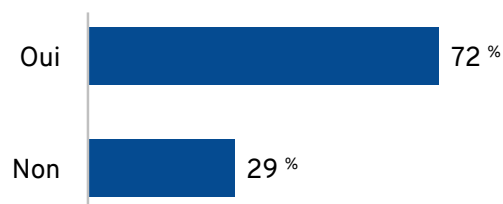
Outre la pression subie par les dirigeants de payer la rançon et passer à autre chose, 64 % des personnes interrogées ont eu le sentiment que l'attaque par ransomware avait eu des répercussions négatives sur la réputation de leur entreprise. De plus, 63 % des collaborateurs et collaboratrices ont indiqué que l'attaque a altéré la confiance qu'ils avaient en leur organisation.

Il n'est donc pas surprenant que selon 26 % des personnes interrogées, l'employeur ait uniquement communiqué l'attaque aux partenaires et clients (et pas au public), tandis que 15 % ne l'ont dit à personne. Ceci traduit le fait que les attaques par ransomware sont probablement beaucoup plus courantes que l'on ne le pense.



Données complètes

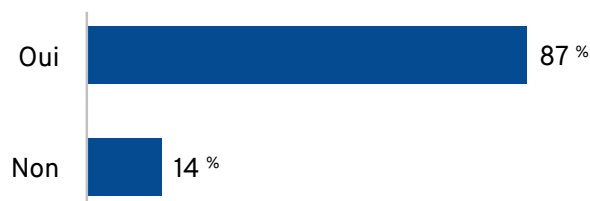
Q1. Avant l'attaque, saviez-vous ce qu'était un ransomware ?



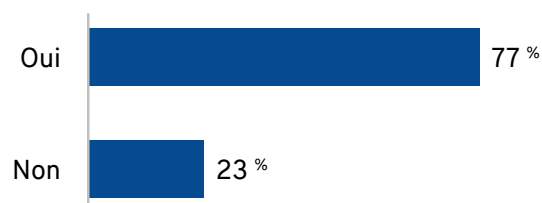
Q2. Quelle était la cause principale de l'attaque par ransomware visant votre entreprise ?



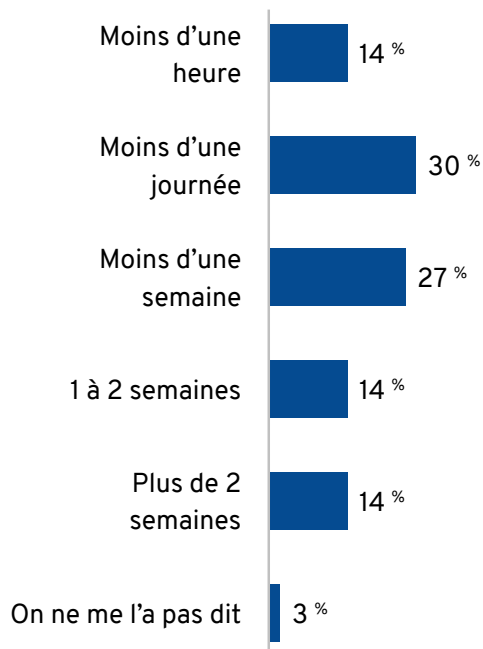
Q3. Votre entreprise a-t-elle adopté des protocoles de sécurité plus stricts à la suite de l'attaque par ransomware ?



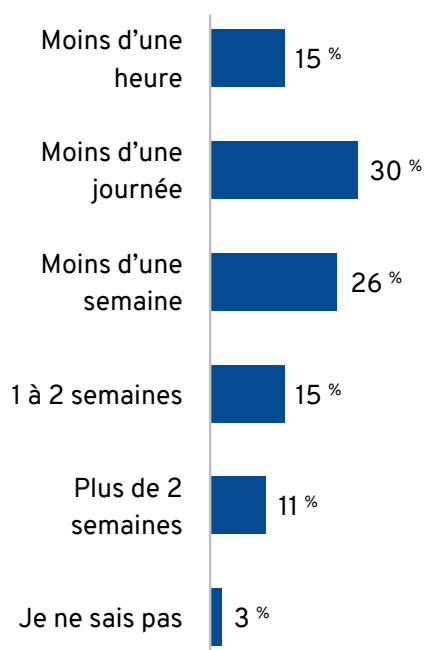
Q4. Votre entreprise a-t-elle été mise hors ligne (p. ex. dans l'incapacité d'accéder aux systèmes ou aux réseaux) en raison de l'attaque par ransomware ?



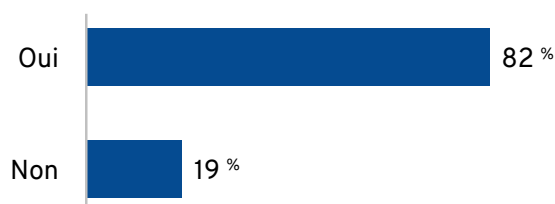
Q5. Si oui, combien de temps votre entreprise a-t-elle été à l'arrêt ?



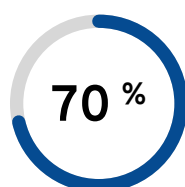
Q6. Si oui, pendant combien de temps avez-vous été dans l'incapacité d'effectuer l'intégralité de vos tâches habituelles ?



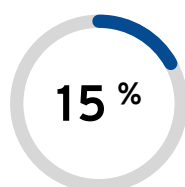
Q7. Trouvez-vous que l'équipe de direction de votre organisation a communiqué efficacement avec son personnel à la suite de l'attaque par ransomware ?



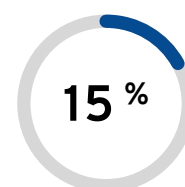
Q8. Votre entreprise a-t-elle alerté sa clientèle et ses partenaires de l'attaque ?



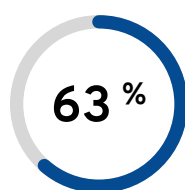
Oui



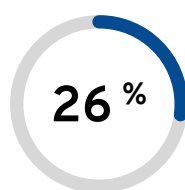
Non



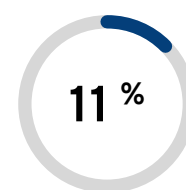
Je ne sais pas

Q9. Votre entreprise a-t-elle publié un communiqué en réaction à l'attaque ?

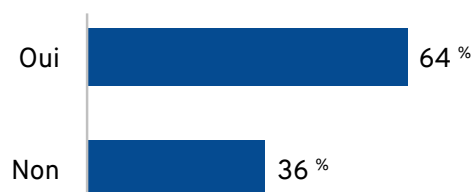
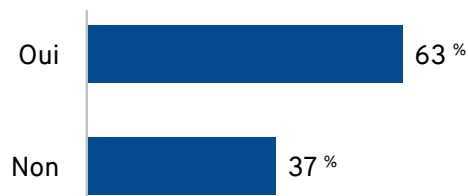
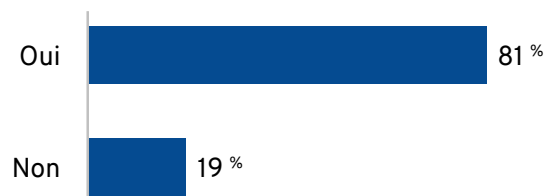
Oui



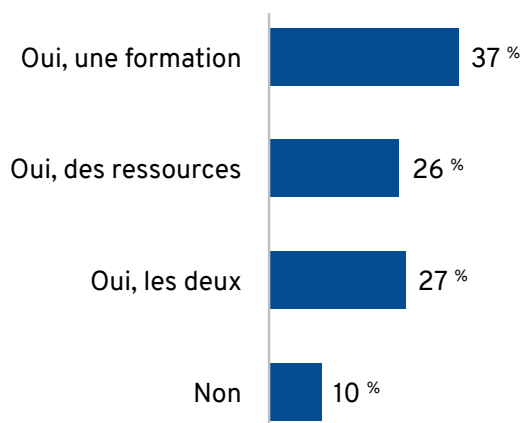
Non



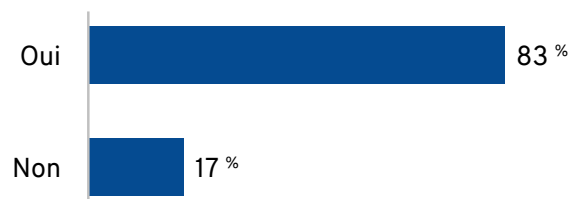
Je ne sais pas

Q10. Avez-vous l'impression que l'attaque par ransomware a affecté la réputation de votre entreprise ?**Q11. L'attaque par ransomware a-t-elle affecté la confiance que vous portez à votre organisation ?****Q12. Avant l'attaque par ransomware, aviez-vous l'habitude d'installer régulièrement les mises à jour logicielles lorsqu'on vous le proposait ?**

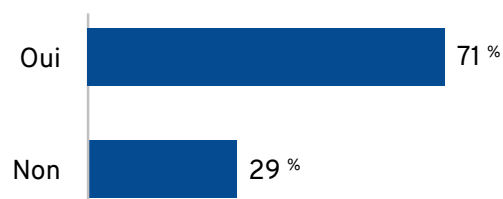
Q13. À la suite de l'attaque, votre entreprise vous a-t-elle fourni une formation ou des ressources liées à la cybersécurité ?



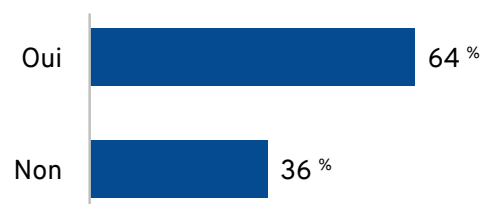
Q14. À la suite de l'attaque, votre entreprise a-t-elle installé des logiciels ou réalisé des améliorations techniques majeures (p. ex. déplacer des éléments vers le cloud) ?



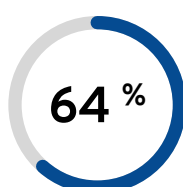
Q15. Si oui, avez-vous trouvé que le processus d'installation de nouveaux logiciels/mises à jour a causé des perturbations ou affecté la productivité ?



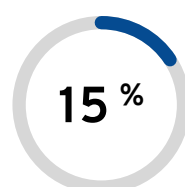
Q16. Si oui, avez-vous perdu des informations, p. ex. des identifiants ou documents de connexion au moment de mettre à jour vos appareils ?



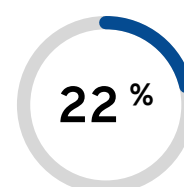
Q17. Le cas échéant, quel a été selon vous l'impact sur vos habitudes de travail quotidiennes ?



Positif

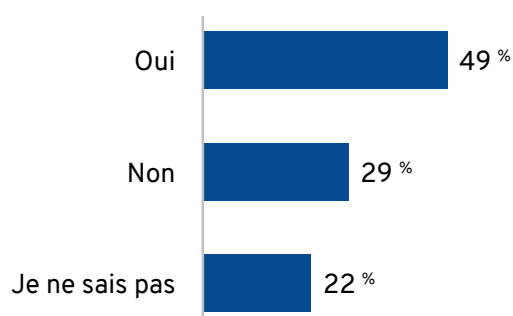


Négatif

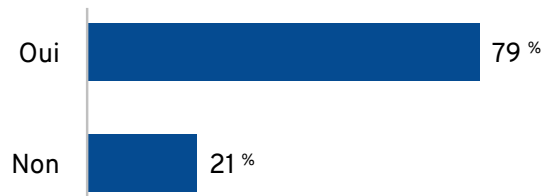


Pas du tout

Q18. Votre entreprise a-t-elle payé la rançon ?



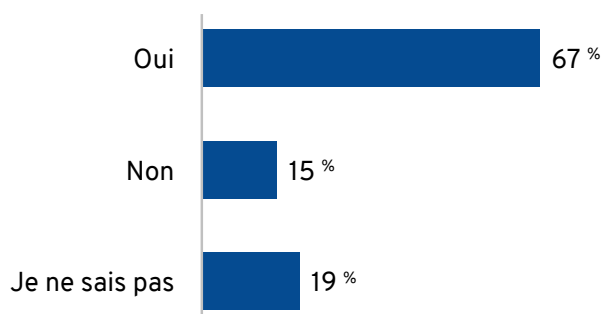
Q19. Si oui, le montant de la rançon a-t-il été communiqué aux employés ?



Q20. Le cas échéant, avez-vous remarqué que votre entreprise réduisait le budget d'autres postes à la suite du paiement ?



Q21. Les dépenses en matière de cybersécurité au sein de votre entreprise ont-elles augmenté après l'attaque ?



À propos de Keeper

Keeper protège les entreprises contre les attaques par ransomware grâce avec des fonctionnalités performantes d'administration, de contrôles et de visibilité pour assurer la sécurité des mots de passe et une analyse en temps réel du dark web.

La plateforme de sécurité et de chiffrement zero-knowledge de Keeper aide des milliers d'entreprises dans le monde à éviter des cyberattaques liées aux mots de passe, à améliorer leur productivité et respecter la conformité.

Keeper offre aux administrateurs informatiques une visibilité complète sur les pratiques de mots de passe du personnel. Ils peuvent ainsi surveiller le respect des exigences et des politiques de sécurité des mots de passe sur l'ensemble de l'organisation, notamment avec la mise en place de mots de passe forts et uniques et d'une authentification multi-facteurs (2FA). Les contrôles d'accès en fonction du rôle permettent aux administrateurs de définir des permissions pour les collaborateurs en fonction de leurs rôles et responsabilités, et de mettre en place des dossiers partagés pour certains groupes, par exemple par classification de poste ou équipe de projets.

Pour une protection encore plus sûre, les organisations peuvent déployer des outils complémentaires comme Keeper Secure File Storage, qui permet au personnel d'enregistrer et partager en toute sécurité des documents, images, vidéos et même des certificats numériques et clés SSH, ou BreachWatch™, qui scanne les forums du dark web et alerte les administrateurs informatiques si les mots de passe des employés ont été piratés lors d'une violation de données publique.

Keeper est certifié SOC-2, FIPS 140-2 et ISO 27001 et figure sur la liste autorisée du gouvernement fédéral américain via le System for Award Management (SAM). Keeper protège les petites et grandes entreprises des principaux secteurs industriels.

Rendez-vous sur keeper.io/ransomware-impact pour obtenir de plus amples informations.

