EBOOK

5 raisons pour lesquelles il est impossible de prévenir les ransomware

NetApp

Sommaire

5 C'est rentable

4 Cela ne coûte pas cher

3 Cela est reconnu comme efficace

2 Cela offre un ROI rapide

1 Les utilisateurs ne sont pas fiables

Protection Zero trust contre les ransomware

Au vu du nombre d'attaques de ransomware à grand retentissement de ces dernières années et de la gravité des conséquences d'une infection, on pourrait penser que les méthodes de prévention auront bientôt assez mûri pour éradiquer les ransomware.

Songez à la menace autrefois omniprésente des kits d'exploit, comme le tristement célèbre Angler, qui constituait à l'époque un énorme casse-tête pour les équipes de sécurité. Grâce aux efforts incessants des chercheurs pour les combattre, ils ne sont pratiquement plus qu'un lointain souvenir.

Mais les ransomware sont toujours là, et il est impossible de les prévenir totalement. Voyons pourquoi c'est toujours le cas.

5

C'est rentable

Les pirates sont plus motivés que jamais, car une attaque réussie génère d'énormes bénéfices. Le montant moyen des rançons payées par les entreprises situées aux États-Unis, au Canada et en Europe est passé de 115 123 $ en 2019 à 312 493 $ en 2020, soit une augmentation annuelle de 171 %. Le montant moyen au premier trimestre de l'exercice fiscal 2021 s'élevait à 850 000 $. Depuis 2019, les incidents liés à des ransomware ont augmenté de 65 %. Les attaques seront de plus en plus fréquentes. Au lieu d'une attaque toutes les 11 secondes, on estime qu'une attaque se produira toutes les 2 secondes d'ici 2031. Elles deviendront donc monnaie courante. Avec de tels chiffres, on comprend pourquoi le ransomware continue d'être l'une des activités les plus prisées des criminels.

Et même si les autorités le déconseillent, les entreprises continuent de payer les rançons. Il est naturel que les entreprises veuillent protéger leurs données, mais le coût de la perturbation de l'activité est souvent supérieur à la rançon elle-même. Payer est souvent l'option la plus économique.

4

Cela ne coûte pas cher

Inversement, les coûts d'organisation d'une campagne de ransomware sont faibles. Aujourd'hui, un malfaiteur peut acheter un kit de ransomware pour une somme relativement modique. Le kit contient tout ce qui est nécessaire pour déployer et monétiser une attaque, y compris les services de chiffrement, l'injecteur de la charge et les outils de brouillage. Le prix d'un abonnement de « ransomware en tant que service » (RaaS) commence généralement à une centaine de dollars par mois. Les variantes plus complexes et plus puissantes peuvent coûter des milliers de dollars, mais le potentiel de gain augmente également. Ces tarifs incluent un support, pour que les attaquants puissent tirer un maximum de valeur du service.

3

Cela est reconnu comme efficace

Les ransomware représentent un business rentable. Oubliez le stéréotype des malfaiteurs en sweat à capuche dans des pièces sombres ; il s'agit d'un réseau sophistiqué comparable à n'importe quel programme de partenariat d'entreprise. L'un des exemples les plus récents de RaaS est DarkSide, qui a été détecté pour la première fois début août 2020 et qui a été intégré dans un modèle de distribution RaaS en novembre. D'après les incidents signalés, la demande de rançon est généralement comprise entre 200 000 $ et 2 millions de dollars pour obtenir les clés permettant de déverrouiller vos données. Les hackers à l'origine de DarkSide ont recueilli de nombreux paiements et se considèrent comme des « Robin des Bois », c'est-à-dire qu'ils ponctionnent l'argent des grandes entreprises fructueuses et reversent leurs recettes sous forme de dons. Des rapports indiquent qu'au moins 90 victimes ont été touchées par DarkSide à ce jour. Au total, plus de 2 To de données volées sont actuellement hébergées sur des sites DarkSide, une autre raison d'inciter au paiement.

2

Cela offre un ROI rapide

Une autre raison pour laquelle les ransomware sont si attrayants est qu'une fois qu'ils se sont introduits dans une entreprise, généralement par le biais de pièces jointes à un e-mail, d'URL malveillantes, de protocoles de postes de travail à distance non sécurisés ou de publicités malveillantes, ils agissent rapidement. Ils analysent le réseau pour localiser les fichiers, puis en chiffrent le contenu et demandent une rançon. Malheureusement, il est très rare de parvenir à annuler le processus de chiffrement a posteriori. Plus inquiétant encore, une nouvelle méthodologie est apparue, consistant à voler les données avant de les chiffrer. En mai 2021, le Colonial Pipeline, fournisseur de 45 % du pétrole pour la côte Est des États-Unis, a subi une attaque par ransomware. Cette attaque a été perpétrée par DarkSide ou une filiale. Outre le verrouillage des systèmes informatiques du Colonial Pipeline, DarkSide a volé plus de 100 Go de données de l'entreprise. Ce vol de données prouve que le groupe extorque doublement ses victimes. Non seulement il réclame de l'argent pour déverrouiller les ordinateurs infectés, mais il demande également à être payé en échange des données volées, tout en menaçant de les divulguer publiquement en cas de refus de paiement.

1

Les utilisateurs ne sont pas fiables

Jusqu'à présent, nous avons vu pourquoi les ransomware étaient si omniprésents, mais nous n'avons rien dit sur la façon de les arrêter. S'il est vrai qu'un grand nombre d'attaques pourraient être évitées avec une meilleure hygiène en matière de correctifs, une raison de poids empêche une prévention absolue : le facteur humain.

Vous avez la conviction que vos employés ne nuiront jamais intentionnellement à votre organisation. Cependant, les infections par ransomware sont toujours d'actualité, car les utilisateurs ne sont pas suffisamment vigilants sur les dangers des liens et e-mails malveillants ou des tentatives de phishing.

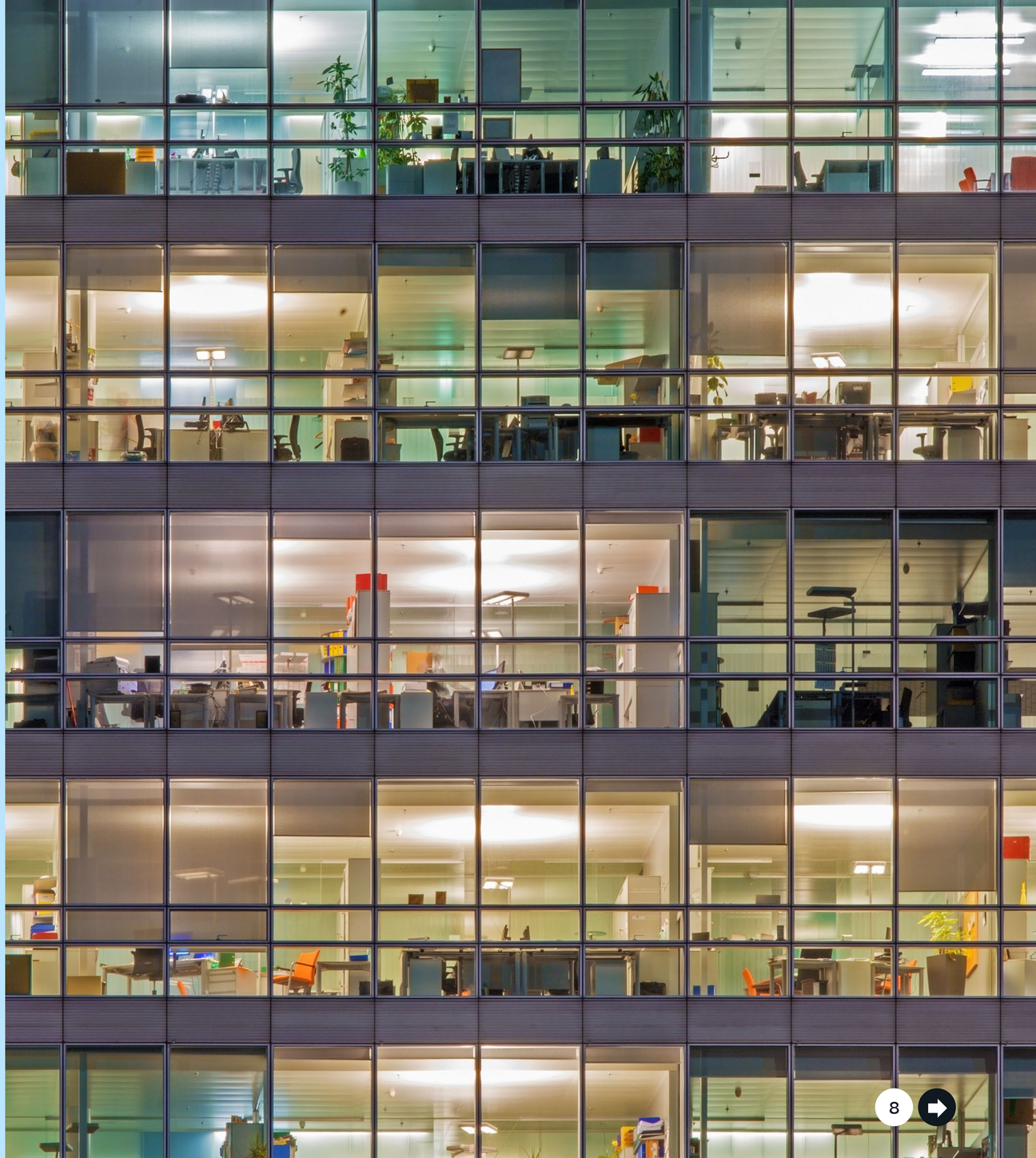
Nombre d'entre eux connaissent certainement les formations régulières obligatoires de sensibilisation à la sécurité. La formation ne fait pas de mal, mais même vos employés les plus sensibilisés à la sécurité peuvent avoir un moment d'inattention en cliquant sur un lien ou en ouvrant un e-mail. Sans politiques de sécurité ultra restrictives qui gênent le personnel dans son travail, une telle erreur de jugement est suffisante. Il convient de détecter les attaques en quelques secondes, non pas en plusieurs minutes ou heures.

Protection Zero trust contre les ransomware

Si vous ne pouvez pas empêcher les ransomware, que pouvez-vous faire pour vous en protéger ?

Vos employés ont besoin d'accéder aux données pour faire leur travail, tout comme les ransomware. Ils deviennent donc le vecteur de l'attaque. Les politiques et les rôles qui limitent l'accès aux données sont utiles. Trop nombreux, ils peuvent cependant nuire à la productivité.

La réponse est la détection précoce, l'analyse du comportement des utilisateurs et l'action automatisée dès que des phénomènes suspects apparaissent. Et ce, en quelques secondes.



NetApp® Cloud Insights offre exactement ce type de détection grâce à une fonctionnalité appelée Cloud Secure. Avec Cloud Secure, vous pouvez surveiller l'activité, détecter les anomalies et automatiser les réponses.

- **Surveillance de l'activité des utilisateurs**
  Pour identifier avec précision les violations d'accès, les activités de chaque utilisateur survenant dans les environnements de Cloud hybride et sur site sont capturées et analysées. En effet, un agent léger installé sur une machine virtuelle dans l'environnement du client collecte les données. Il s'agit notamment des données utilisateur des serveurs Active Directory et LDAP ainsi que des activités des utilisateurs sur les fichiers liées au stockage NetApp ONTAP®, soit dans vos propres data centers, soit dans le cloud.

  Cloud Secure détecte les comportements d'utilisation anormaux en créant un modèle comportemental pour chaque utilisateur. Il se sert de ce modèle pour détecter les activités anormales des utilisateurs puis les analyse pour déterminer si la menace est de type ransomware ou si elle provient d'un utilisateur malveillant. Ce modèle comportemental réduit les faux positifs.

- **Détection des anomalies et identification des attaques potentielles**
  Les attaques par ransomware et malware sont aujourd'hui très sophistiquées et difficilement détectables par les solutions basées sur les signatures (liste rouge), car elles utilisent des extensions et noms de fichiers aléatoires. Basée sur des algorithmes avancés de machine learning, la fonctionnalité Cloud Secure est quant à elle en mesure de détecter toute activité de données inhabituelle et toute attaque éventuelle. Cette détection à la fois dynamique et précise réduit le nombre de faux positifs.

- **Automatisation des politiques de réponse**
  Cloud Secure vous signale une attaque potentielle par ransomware et propose plusieurs politiques de réponse automatiques pour protéger vos données contre cette attaque.

  Une copie NetApp Snapshot™ est créée en présence d'un comportement inhabituel. Vos données sont protégées pour vous permettre de récupérer rapidement, tout en limitant le nombre d'interruptions potentielles liées à un faux positif.

Bloquez l'accès d'un utilisateur à des données :
- Si un comportement anormal (lecture/écriture) est détecté.
- Si une suppression de fichier inhabituelle est détectée.

Cloud Secure propose un audit détaillé des accès pour permettre aux administrateurs d'identifier rapidement les données compromises ainsi que la source de l'attaque afin d'accélérer la résolution des problèmes et la reprise.

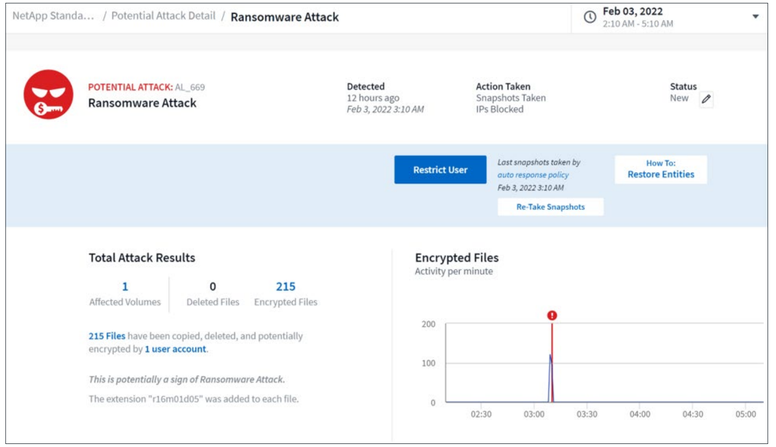


Figure 1) Tableau de bord Cloud Secure indiquant une attaque par ransomware.

Si vous souhaitez en savoir plus sur Cloud Secure, inscrivez-vous à notre essai gratuit de 30 jours. **En savoir plus et essayer gratuitement.**

À propos de NetApp

In a world full of generalists, NetApp is a specialist. We're focused on one thing, helping your business get the most out of your data. NetApp brings the enterprise-grade data services you rely on into the cloud, and the simple flexibility of cloud into the data center. Our industry-leading solutions work across diverse customer environments and the world's biggest public clouds.

En tant qu'entreprise spécialisée dans les logiciels et axée sur le cloud et les données, seul NetApp peut vous aider à créer votre propre Data Fabric, à simplifier et connecter votre cloud, et à fournir les données, les applications et les services adaptés aux personnes appropriées, en tout lieu et à tout moment.

NetApp