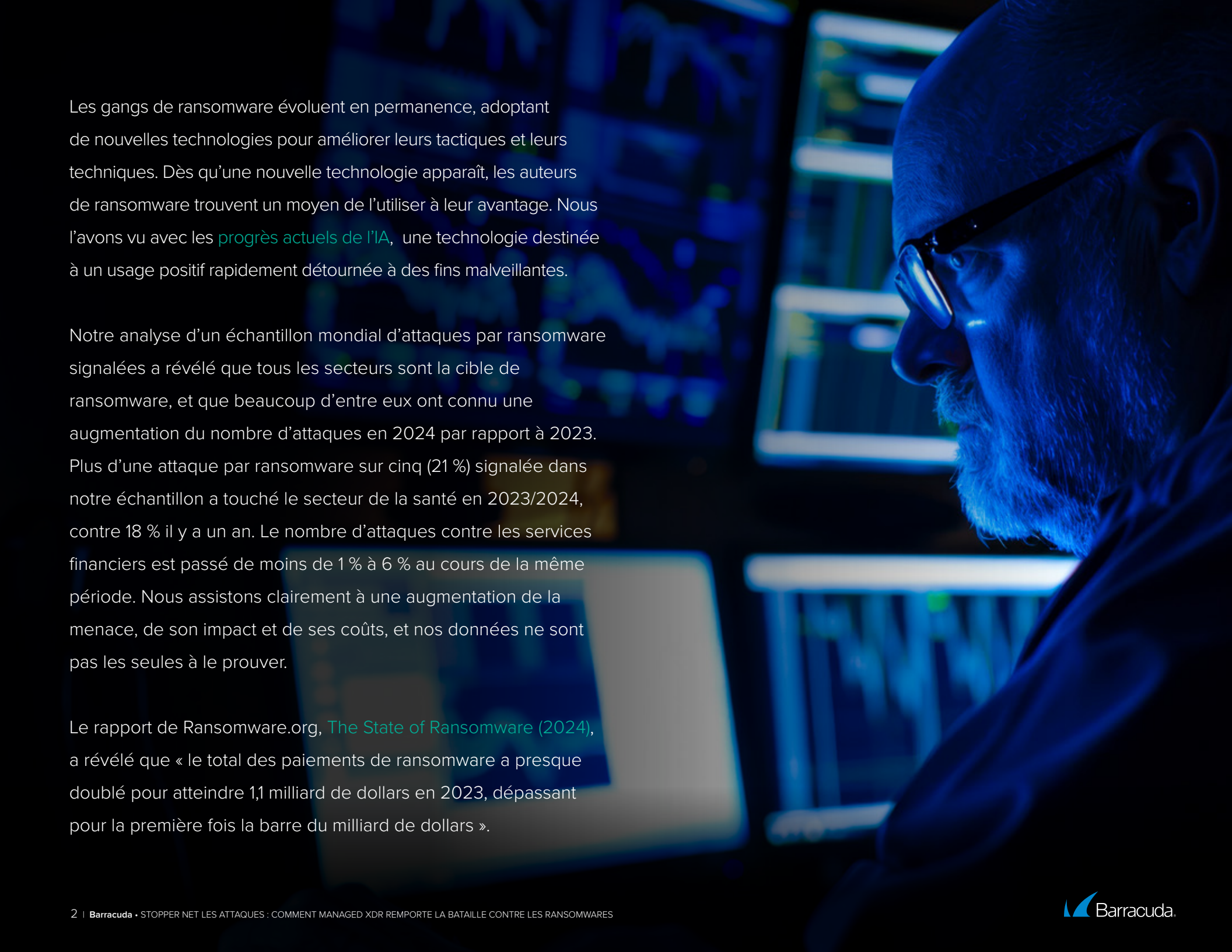
# Stopper net les attaques : comment Managed XDR remporte la bataille contre les ransomwares

Barracuda



Les gangs de ransomware évoluent en permanence, adoptant de nouvelles technologies pour améliorer leurs tactiques et leurs techniques. Dès qu'une nouvelle technologie apparaît, les auteurs de ransomware trouvent un moyen de l'utiliser à leur avantage. Nous l'avons vu avec les progrès actuels de l'IA, une technologie destinée à un usage positif rapidement détournée à des fins malveillantes.

Notre analyse d'un échantillon mondial d'attaques par ransomware signalées a révélé que tous les secteurs sont la cible de ransomware, et que beaucoup d'entre eux ont connu une augmentation du nombre d'attaques en 2024 par rapport à 2023. Plus d'une attaque par ransomware sur cinq (21 %) signalée dans notre échantillon a touché le secteur de la santé en 2023/2024, contre 18 % il y a un an. Le nombre d'attaques contre les services financiers est passé de moins de 1 % à 6 % au cours de la même période. Nous assistons clairement à une augmentation de la menace, de son impact et de ses coûts, et nos données ne sont pas les seules à le prouver.

Le rapport de Ransomware.org, The State of Ransomware (2024), a révélé que « le total des paiements de ransomware a presque doublé pour atteindre 1,1 milliard de dollars en 2023, dépassant pour la première fois la barre du milliard de dollars ».

# Comment les attaques par ransomware s'introduisent-elles dans les organisations ?

Les tactiques et points d'entrée utilisés par les pirates pour pénétrer dans les organisations sont nombreux. De nombreux attaquants tentent plusieurs approches simultanément jusqu'à ce qu'ils réussissent à s'introduire dans le réseau cible. Voici quelques-unes de ces tactiques :

**Phishing/vishing/quishing/smishing**

Ces techniques utilisent respectivement les comptes e-mail, les appels et messages vocaux, les codes QR et les SMS. Ces attaques consistent à envoyer des liens malveillants à une personne cible, généralement sur son compte ou son appareil professionnel. L'objectif est d'amener l'utilisateur à cliquer sur un lien et à saisir des informations de connexion, que les pirates peuvent ensuite utiliser pour pénétrer dans le réseau ou pour amener les victimes à télécharger des pièces jointes malveillantes.

**Exploiter des vulnérabilités logicielles non corrigées ou inconnues (zero-day)**

Parfois, un pirate parvient à identifier une vulnérabilité dans un logiciel avant le fournisseur ou l'organisation, ce qui lui permet d'exploiter la vulnérabilité non corrigée et d'insérer un code malveillant qui lui permet de dérober des données. C'est ce qu'on appelle une attaque de type zero-day. De plus, les gangs de ransomware analysent activement les réseaux à la recherche de vulnérabilités connues qui n'ont pas encore été corrigées pour en faire la cible d'une attaque.



Barracuda

### Matériel infecté

Certains attaquants utilisent des méthodes plus traditionnelles, telles que l'envoi de périphériques infectés à une entreprise, comme des clés USB contenant un ransomware qui se propage ensuite dans les fichiers cibles et les chiffre. L'attaquant demande alors une rançon pour déchiffrer les données.

### Les attaques contre les chaînes logistiques

Les attaques de la chaîne d'approvisionnement ciblent un fournisseur ou un service tiers dont dépend une entreprise, en ajoutant un code malveillant à son logiciel. Ensuite, lorsque le fournisseur envoie une mise à jour, le malware se propage au sein de l'organisation ciblée, lançant une attaque de ransomware indirecte.

### Acteurs malveillants en interne

Certaines attaques par ransomware proviennent de l'intérieur de l'organisation, par le biais de ce que l'on appelle communément un acteur malveillant en interne. Il s'agit d'une personne encouragée par un gang de ransomware (ou qui dirige elle-même une opération de ransomware) qui utilise son accès privilégié pour compromettre l'entreprise pour laquelle elle travaille.

Il ne s'agit là que de quelques-uns des moyens utilisés par les auteurs de ransomwares pour pénétrer dans une organisation, et les pirates développent sans cesse de nouvelles méthodes. Pour conceptualiser l'approche de défense de tous ces points d'entrée, on peut établir une comparaison avec la sécurité d'une maison. Un système de sécurité domestique complet comprenant une vidéosurveillance, des alarmes de détection d'intrusion, des systèmes de verrouillage avancés et des alertes automatisées est bien plus efficace qu'un système reposant uniquement sur le verrouillage des portes. La combinaison de la détection et de la réaction dans votre stratégie de sécurité, en plus des méthodes de défense plus traditionnelles, permet d'assurer une bien meilleure protection.

# Les organisations sont-elles prêtes à répondre aux attaques par ransomware ?

La capacité à répondre à une attaque par ransomware dépend de la maturité de la stratégie de réponse aux menaces d'une organisation. Les capacités des cyberattaquants étant de plus en plus sophistiquées, cette stratégie doit évoluer en fonction de l'évolution des tactiques des acteurs malveillants. Le rapport Ransomware.org cité précédemment a révélé que seulement 14 % des personnes interrogées affirment être entièrement préparées grâce à des plans de réponse testés. Environ 35 % des organisations ont déclaré qu'elles étaient partiellement préparées mais qu'elles avaient quelques lacunes, et 15 % ont reconnu qu'elles n'étaient pas préparées. Avec 86 % des personnes interrogées déclarant ne pas être totalement préparées, il ne fait aucun doute qu'une grande partie des entreprises doivent adopter de nouvelles défenses plus solides pour se protéger contre les ransomwares.



Barracuda.

# Présentation de la détection et de la réponse étendues managées (XDR)

Renforcer les systèmes de détection et de réponse de votre organisation est un moyen fiable d'améliorer l'efficacité de votre stratégie de protection contre les ransomwares. Souvent, les entreprises ne se rendent pas compte que leur sécurité est compromise depuis des mois, ce qui aggrave les dommages et augmente le temps nécessaire pour se rétablir.

**Combien de temps faut-il généralement pour résoudre les compromissions ?**

| | Sans XDR | Avec XDR |
|---|---|---|
| Résolution classique des compromissions d'e-mails professionnels (passerelle uniquement) | 1 à 2 mois | **1 à 2 heures** |
| Résolution de l'usurpation d'identité | 3 à 4 semaines | **1 à 2 heures** |
| Résolution des infections par malware | 3 à 4 semaines | **Environ 1 heure** |
| Résolution des menaces internes | 3 à 6 mois | **Environ 4 heures** |
| Résolution des cas d'extorsion sans XDR | Variable | **< 24 heures** |



Barracuda

Cependant, les équipes de sécurité de nombreuses organisations sont déjà confrontées à des contraintes de temps et à de lourdes charges de travail et ne sont pas en mesure d'ajouter de nouvelles responsabilités à une liste de tâches qui ne cesse de s'allonger.

Dans une enquête réalisée en 2022 par Cybersecurity The State of Extended Detection and Response, 52 % des organisations ont déclaré que le manque de personnel de sécurité qualifié était leur principal défi en matière de cybersécurité. La solution, selon Ransomware.org : « Augmentez vos capacités internes de réponse aux ransomwares avec des services sous-traités et/ou managés par des partenaires de confiance ». La mise en œuvre d'une solution XDR managée est un moyen très efficace de bénéficier des capacités complètes de détection et de réponse dont les entreprises ont besoin pour renforcer leur architecture de cybersécurité, en particulier lorsqu'elles manquent de personnel qualifié.

Managed XDR offre un référentiel unique pour les données de sécurité et la télémétrie, ainsi qu'une capacité d'analyse permettant d'exploiter ces données et d'accélérer la détection des menaces. Managed XDR fournit également des réponses automatisées aux incidents basées sur des playbooks et des plans préalablement convenus. Parallèlement, les systèmes de détection et de réponse du réseau collectent et vérifient les journaux des appareils sur le réseau et analysent le trafic entrant, sortant et interne du réseau de l'entreprise.

Managed XDR utilise les données de sécurité générées par chacune de ces sources, ainsi que d'autres. Les analystes de sécurité donnent ensuite un sens à ces données, contiennent les menaces ou fournissent aux organisations des conseils de correction exploitables, accélérant ainsi la détection et les temps de réponse. Cela permet de mieux comprendre la situation et de distinguer les menaces réelles des fausses alertes. Environ 72 % des personnes interrogées dans le cadre de l'enquête réalisée par Cybersecurity Insiders ont convenu qu'une solution XDR managée est une plateforme fondamentale.

# Comment la solution XDR améliore votre niveau de sécurité

La partie détection de XDR donne aux entreprises une visibilité globale accrue sur l'état de leur réseau, ainsi que sur l'ensemble des menaces, qu'elles soient de type ransomware ou autres, qui tentent d'y pénétrer. On peut la comparer à la caméra d'un système de sécurité domestique : elle vous donne une visibilité constante sur ce qui se passe dans votre environnement numérique. Cette « caméra » a une meilleure précision et une plus grande capacité d'analyse des événements qu'un humain vérifiant manuellement les menaces. XDR bloque également les menaces telles que les adresses IP, les domaines et les hachages de fichiers qu'il identifie comme malveillants, tout comme un système de verrouillage solide qui empêche les intrus de pénétrer dans votre domicile.

L'automatisation est un élément clé de la solution XDR. Elle permet d'accélérer considérablement la réponse aux incidents. Le système envoie des réponses et des alertes automatisées, tout comme une solution d'alarme de sécurité domestique, afin de réagir rapidement aux menaces de sécurité et d'informer les personnes concernées. Sa simplicité est un autre avantage clé : nul besoin d'avoir recours à solutions multipoints proposées par différents fournisseurs pour détecter les menaces et y répondre lorsque vous disposez d'une solution XDR managée. Elle simplifie également la création de rapports pour l'analyse des données et la conformité, car elle enregistre toutes les menaces potentielles, les alertes et les réponses automatisées avec un système de rapports centralisé, tout comme les journaux d'historique des événements générés par les systèmes de sécurité domestique. Pour en savoir plus sur le fonctionnement de XDR et ses avantages pour les organisations, consultez notre eBook, Le XDR expliqué : une approche stratégique du management des menaces.

Pour en savoir plus sur la façon dont une solution XDR managée pourrait renforcer la posture de cybersécurité de votre entreprise, visitez notre site Web. Découvrez également comment Barracuda peut accélérer la détection et réduire votre temps de réponse grâce à un service XDR managé 24 h/24, 7 j/7, 365 jours par an.



Barracuda

# Barracuda en quelques mots

Chez Barracuda, nous nous efforçons de rendre le monde plus sûr. Nous pensons que chaque entreprise mérite un accès à des solutions de sécurité de niveau professionnel cloud-first, abordables, intuitives et facilement déployables. Nous protégeons vos e-mails, réseaux, données et applications à l'aide de solutions innovantes capables de s'adapter au parcours de nos clients, et de se développer en conséquence. Des centaines de milliers d'organisations du monde entier font confiance à Barracuda pour les protéger et les soutenir afin qu'elles puissent se concentrer sur leur croissance. Pour en savoir plus, consultez le site fr.barracuda.com.

Barracuda


Barracuda et le logo Barracuda sont des marques déposées de Barracuda, Inc., États-Unis. Tous les autres noms appartiennent à leurs propriétaires respectifs.