SONICWALL®

# 8 MANIÈRES DE PROTÉGER VOTRE RÉSEAU CONTRE LES RANSOMWARES

**Comment prévenir les attaques de ransomware et garder votre argent**

Parfois, l'ancien revient au goût du jour. C'est le cas des attaques par ransomware, qui ont retrouvé leur popularité. Apparus en 1989, les ransomwares infectent un système et « immobilisent » l'utilisateur en lui interdisant d'accéder à l'équipement ou aux fichiers. Une fois que la victime accepte de payer une rançon, habituellement sous la forme de bitcoins, le système est déverrouillé et à nouveau accessible.

L'e-book suivant présente huit manières de protéger votre réseau des attaques par ransomware et d'éviter de donner votre argent aux cybercriminels.

Le montant des rançons varie, mais il se situe souvent entre 200 et 400 dollars.[1]

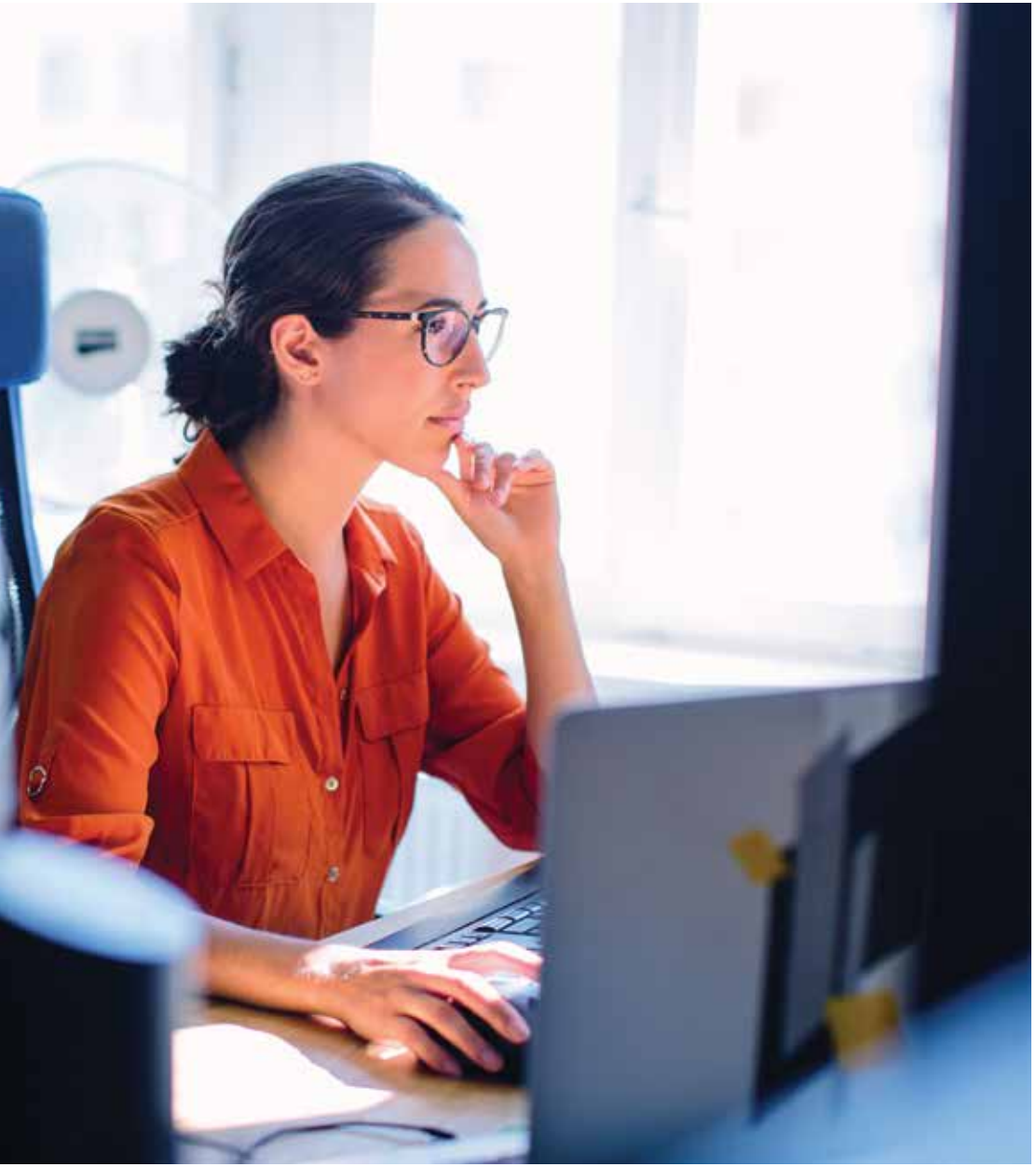

### 1. Éduquez vos employés

L'éducation et la sensibilisation des utilisateurs est fondamentale lorsqu'il s'agit de lutter contre les ransomwares. Considérez avec précaution tous les e-mails suspects. Inspectez le nom du domaine qui a envoyé l'e-mail. Repérez les fautes d'orthographe, inspectez la signature et la légitimité de la demande. Placez la souris sur les liens pour en connaître la destination.

### 2. Utilisez une approche multicouche de la sécurité réseau

La protection contre les ransomwares et les autres formes de programmes malveillants ne commence et ne s'arrête pas à la passerelle.  Pour étendre la sécurité, il est essentiel d'utiliser antivirus, anti-spyware, prévention des intrusions et autres technologies pour les équipements situés sur le périmètre réseau.  Adoptez une approche multicouche permettant de bloquer les ransomwares en éliminant tout point de défaillance dans votre architecture de sécurité

*1 US Computer Emergency Readiness Team Alert (TA16-091A)*



### 3. Sauvegardez régulièrement vos fichiers

L'autre façon de se prémunir contre le paiement d'une rançon consiste à établir une solide stratégie de sauvegarde et de récupération. Selon la rapidité avec laquelle l'attaque est détectée, selon l'étendue de la propagation et le niveau acceptable de perte de données, la récupération depuis une sauvegarde peut être une bonne option. Cela demande toutefois une stratégie de sauvegarde mieux réfléchie, alignée sur le degré de confidentialité de vos données et les besoins de votre entreprise par rapport aux objectifs RPO (perte de données maximale admissible) et RTO (durée maximale d'interruption admissible).

### 4. Veillez à ce que vos terminaux soient protégés

Étant donné que la plupart des utilisateurs interagissent principalement avec des appareils personnels ou professionnels, les terminaux sont particulièrement vulnérables s'ils ne sont pas gérés ou s'ils ne sont pas dotés de la protection anti-malware appropriée. La plupart des solutions antivirus sont basées sur les signatures et s'avèrent inefficaces si elles ne font pas l'objet de mises à jour régulières. Les nouvelles variantes de ransomwares sont codées de manière unique et sont donc indétectables à l'aide des techniques ayant recours aux signatures. Aussi, beaucoup d'utilisateurs désactivent l'analyse antivirus de leur système afin de ne pas ralentir ses performances.

## Mettez en place une stratégie de sécurité multicouche pour mieux protéger votre réseau.

### 5. Appliquez les correctifs à vos systèmes et applications

De nombreuses attaques reposent sur des vulnérabilités connues des navigateurs, notamment Internet Explorer, ainsi que des applications et plug-ins courants. Il est donc fondamental d'appliquer les mises à jour et correctifs de manière rapide et fiable. Le choix d'une solution capable d'automatiser les correctifs et les mises à niveau de versions dans un environnement hétérogène composés de divers appareils, systèmes d'exploitation et applications, est important pour apporter une réponse adéquate à la palette de cyber menaces dont font partie les ransomwares.

### 6. Segmentez votre réseau pour bloquer toute propagation

La plupart des ransomwares vont essayer de se propager depuis le terminal vers le serveur/stockage sur lequel résident toutes les données et applications stratégiques. La segmentation du réseau et l'isolement des applications et appareils sensibles sur un réseau distinct ou un LAN virtuel permet de limiter la propagation.

### 7. Mettez en quarantaine et analysez les fichiers suspects

Les technologies comme le sandboxing offrent la possibilité de déplacer les fichiers suspects en quarantaine afin de les analyser avant qu'ils ne puissent pénétrer sur le réseau. Les fichiers sont retenus au niveau de la passerelle jusqu'à ce qu'un verdict soit rendu. Si un fichier est identifié comme étant suspect, vous pouvez empêcher une infiltration plus poussée à l'aide de mesures de protection telles que des règles bloquant adresses IP ou domaines ou via le déploiement de signatures sur les appliances de sécurité du réseau.

Segmentez votre LAN sans fil pour séparer les utilisateurs internes des utilisateurs invités et améliorer le niveau de sécurité.

### 8. Protégez vos appareils Android

Les appareils utilisant le système d'exploitation Google Android sont devenus les principales cibles des attaques par ransomware. Prenez les mesures suivantes pour protéger votre smartphone Android :

- Ne pas rooter l'appareil, cela expose les fichiers système aux modifications.
- Toujours installer les applications depuis Google Play. Celles provenant de sites/boutiques inconnus peuvent être fausses/malveillantes..
- Désactiver l'installation des applications provenant de sources inconnues.
- Autoriser Google à rechercher les menaces sur l'appareil.
- Prendre garde lors de l'ouverture de liens inconnus reçus dans des SMS ou des e-mails..
- Installer des applications de sécurité tierces qui analysent l'appareil régulièrement afin de détecter des contenus malveillants.
- Surveiller les applications sont enregistrées au titre d'administrateur de l'appareil..
- Pour les appareils de l'entreprise, créer une liste noire d'applications non autorisées.

Les programmes malveillants conçus pour l'écosystème Android ont continué à se développer en 2015, ce qui représente un danger pour près de 85 pour cent des smartphones.

## Conclusion

Les attaques par ransomware connaissent une popularité croissante auprès des cybercriminels. Veillez à ce que votre réseau soit protégé. SonicWall peut améliorer la protection de l'ensemble de votre structure en inspectant chaque paquet et en gouvernant chaque identité. Par conséquent, vos données seront protégées, où qu'elles se trouvent, et les mesures de sauvegarde seront partagées pour de nombreuses menaces, y compris les ransomwares.

Consultez la page Web des produits de sécurité réseau SonicWall.

## À propos de SonicWall

SonicWall s'engage depuis plus de 25 ans dans la lutte contre la cybercriminalité, défendant PME et grands comptes dans le monde entier. Notre alliance de produits et de partenaires nous a permis de mettre sur pied une solution de cyberdéfense en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 150 pays, leur permettant de se concentrer sans crainte sur leur cœur de métier.

Pour toute question concernant l'usage potentiel de ce document, contactez :

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Consultez notre site Internet pour de plus amples informations.
**www.sonicwall.com**







Ebook-8waysRansomware-EU-IMAG-29271-D1

SONICWALL®