SONICWALL

COMMENT UN RANSOMWARE PEUT PRENDRE VOTRE ENTREPRISE EN OTAGE

Comprendre les attaques de ransomwares et leur mode de fonctionnement

Introduction

Un ransomware est une forme de programme malveillant qui bloque l'accès à des données ou systèmes jusqu'à ce que la victime ait payé une rançon au cybercriminel pour que celui-ci lève la restriction. S'ils existent déjà depuis de nombreuses années, ils ont sensiblement gagné en popularité et en rentabilité ces derniers temps. CryptoLocker, CryptoWall et RSA4096 sont des exemples bien connus de ransomwares.

Selon le FBI, plus de 209 millions de dollars ont déjà été versés au cours des trois premiers mois de 2016[1] aux États-Unis, contre 25 millions de dollars de rançons sur toute l'année dernière.

1 http://sd18.senate.ca.gov/news/4122016-bill-outlawing-ransomware-passes-senate-committee

Comment fonctionne un ransomware

Un ransomware peut s'infiltrer dans un système de différentes manières, mais c'est la victime qui, au final, télécharge et installe une application malveillante. Une fois sur l'appareil, l'application se propage partout et chiffre des fichiers sur le disque dur ou verrouille tout simplement le système. Dans certains cas, le blocage se fait par l'affichage à l'écran d'images ou d'un message intimant l'utilisateur de payer une rançon au pirate en échange de la clé de déchiffrement qui lui permettra de déverrouiller les fichiers ou le système.

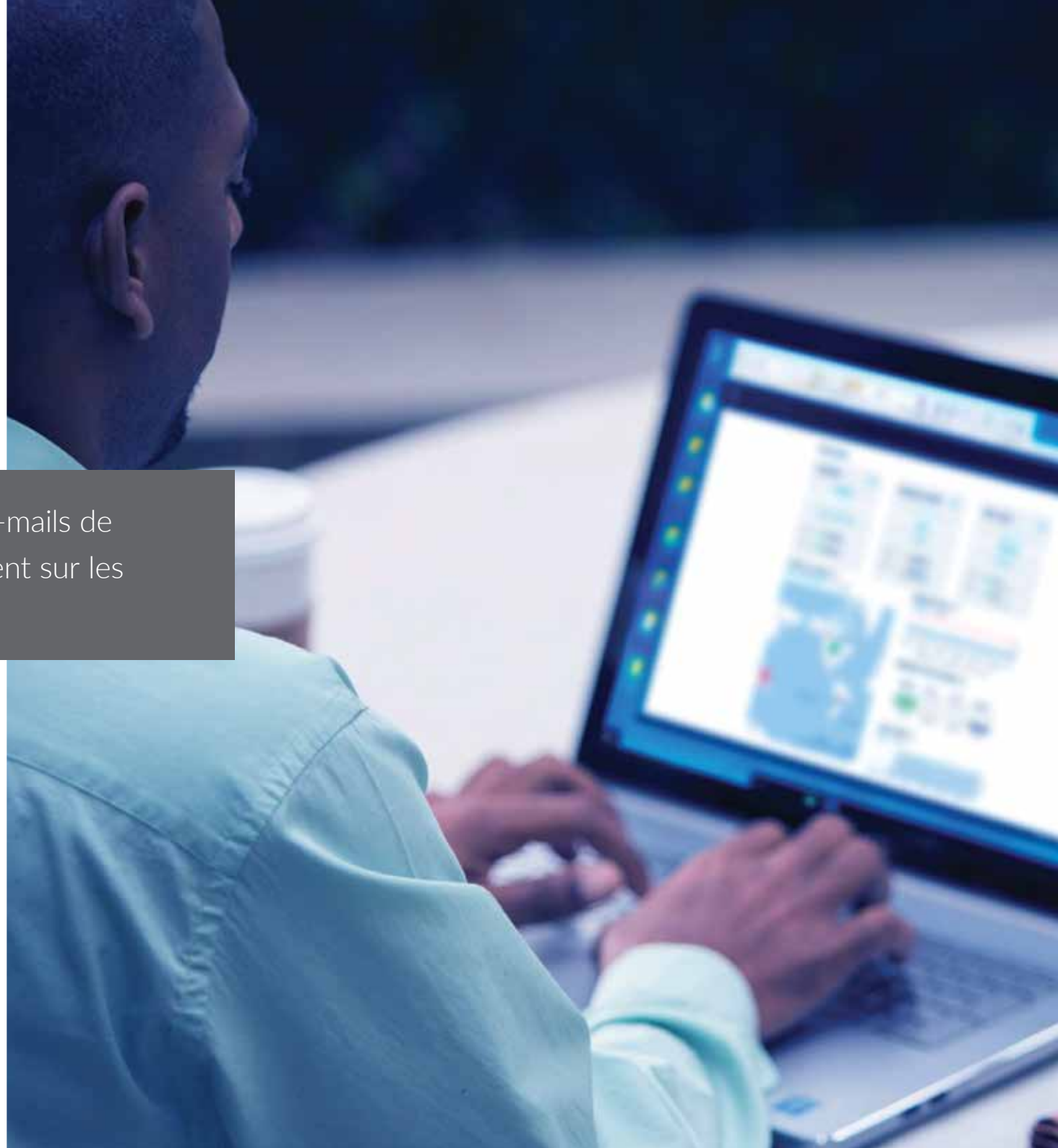
Les bitcoins sont une forme courante de paiement d'une rançon, la monnaie numérique étant difficile à tracer.

SONICWALL®

Phishing

Le phishing est l'une des méthodes les plus courantes de diffusion de ransomware. Les e-mails en question incitent les destinataires à ouvrir un message et à cliquer sur un lien conduisant à un site Web. Le site peut demander des informations confidentielles ou contenir un programme malveillant, un ransomware par exemple, qui se télécharge sur le système de la victime.

23 % des destinataires ouvrent des e-mails de phishing et 11 % cliquent effectivement sur les pièces jointes[2].

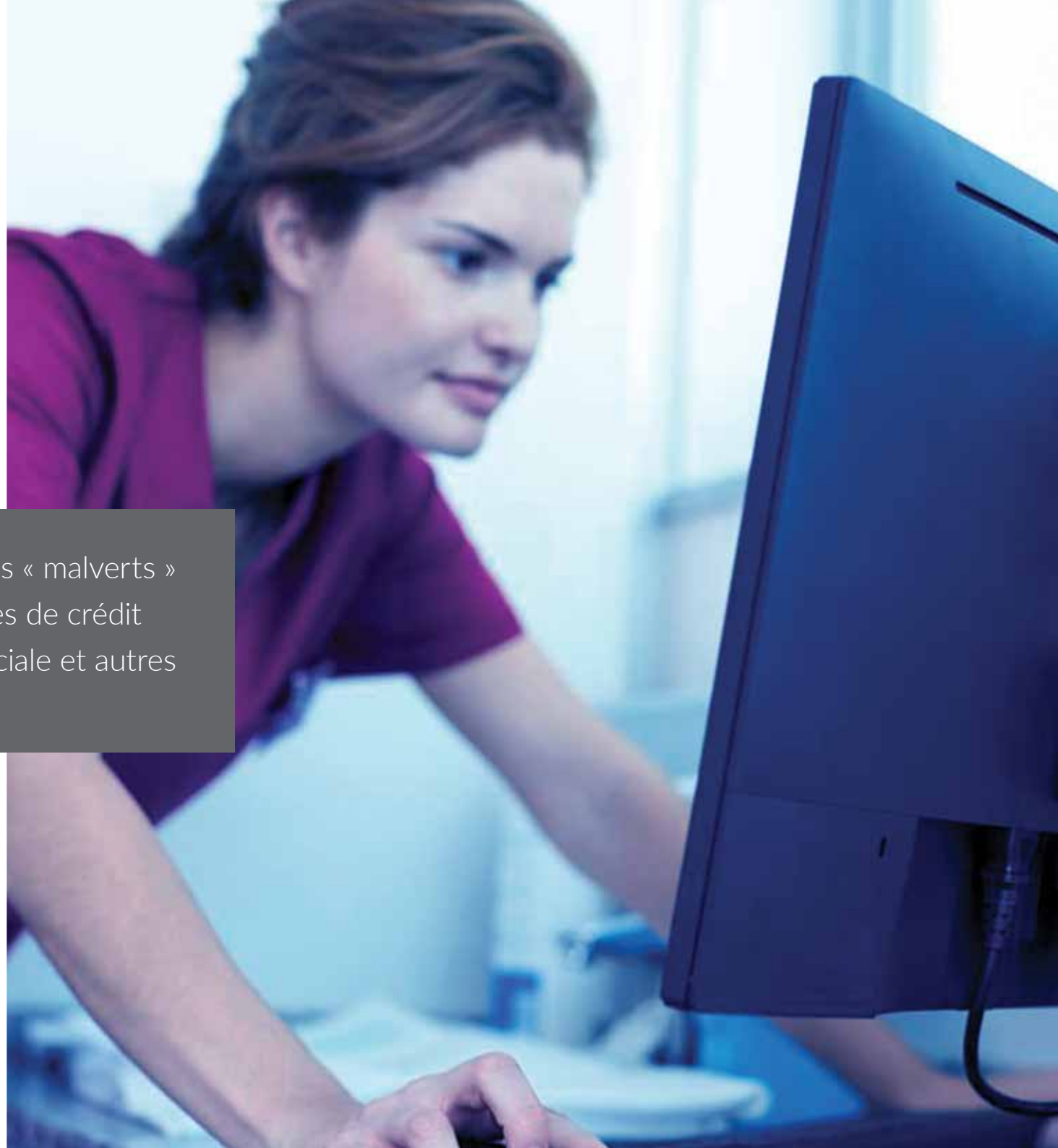


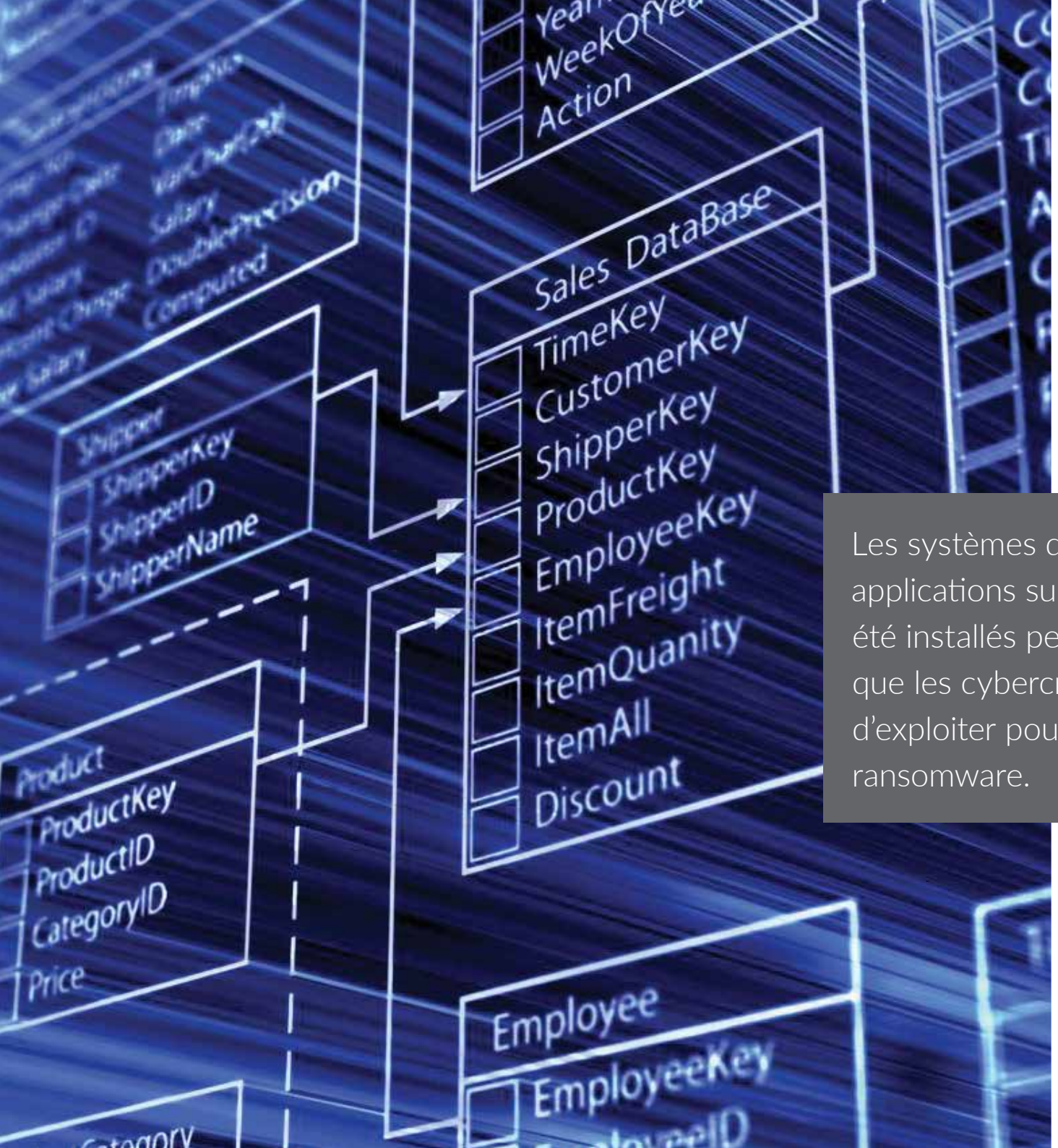
2 2015 Verizon Data Breach Investigation Report

Malvertising

Une autre forme répandue de diffusion de ransomware est ce qu'on appelle le « malvertising » ou publicité malveillante. L'agresseur s'infiltre sur les réseaux publicitaires, se faisant parfois passer pour un faux annonceur ou une fausse agence, et insère des publicités infectées sur des sites Web légitimes. Les visiteurs, qui ne se doutent de rien, n'ont même pas besoin de cliquer sur la publicité pour que leur système soit infecté.

En plus de lancer des ransomwares, les « malverts » peuvent soutirer les numéros de cartes de crédit de clients, les numéros de sécurité sociale et autres informations confidentielles.



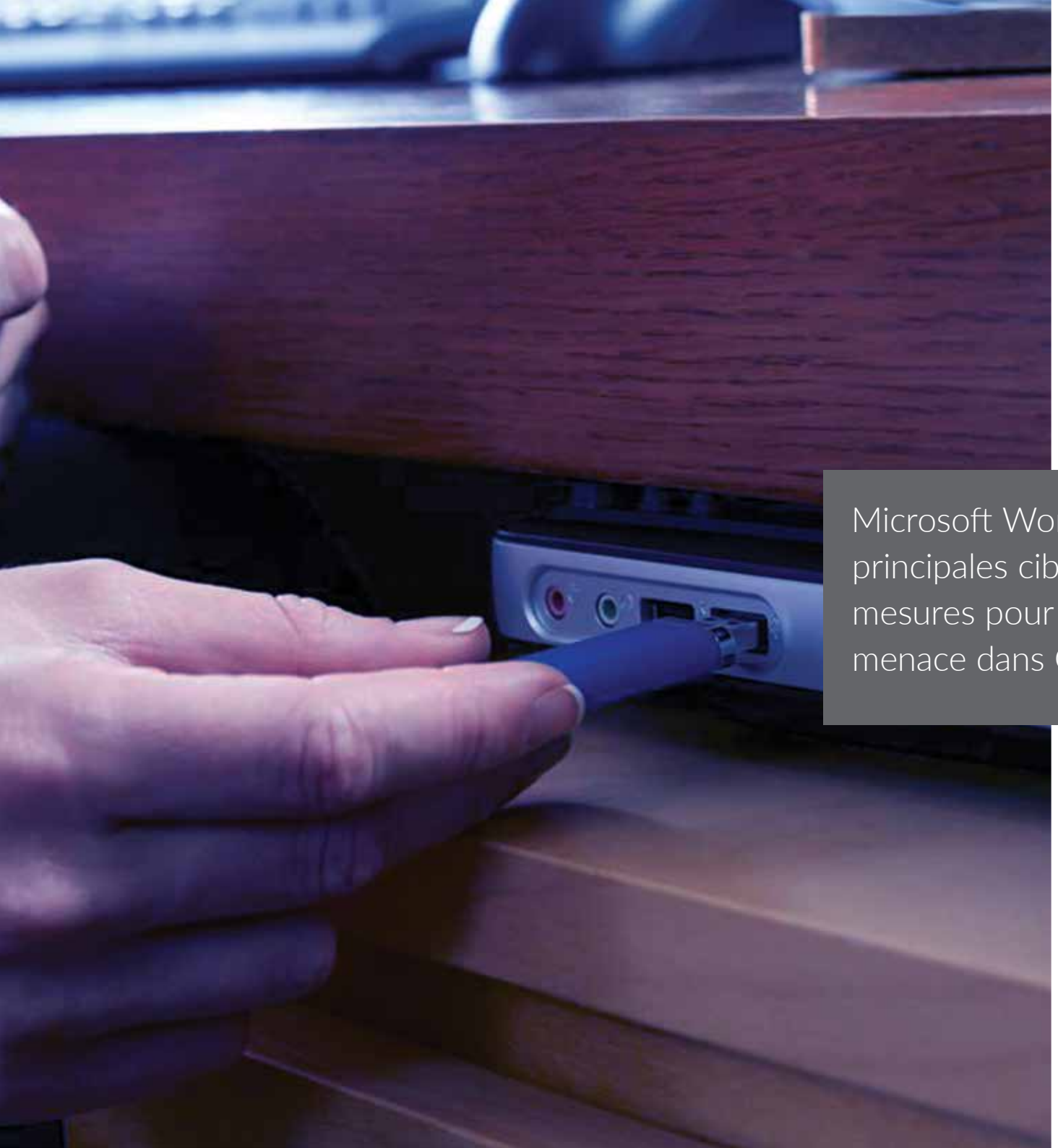


Exploitation de systèmes et d'applications sans correctifs

Bon nombre d'attaques s'appuient sur des vulnérabilités connues des systèmes d'exploitation, des navigateurs et des applications courantes. Les cybercriminels peuvent exploiter ces vulnérabilités pour lancer leur attaque de ransomware, si les systèmes ne sont pas à jour en termes de correctifs logiciels.

Les systèmes d'exploitation, navigateurs et applications sur lesquels les correctifs n'ont pas été installés peuvent contenir des vulnérabilités que les cybercriminels ne manqueront pas d'exploiter pour lancer leurs attaques de ransomware.

SONICWALL®



Périphériques externes

Les périphériques externes, clés USB par exemple, sont utilisés pour stocker et transférer des fichiers, ce qui en fait des cibles privilégiées pour propager des ransomwares à travers plusieurs systèmes. Certains des fichiers contiennent une fonctionnalité avancée, des macros, qui peuvent être utilisées par les hackers pour exécuter un programme à l'ouverture du fichier.

Microsoft Word, Excel et PowerPoint sont les principales cibles, même si Microsoft a pris des mesures pour renforcer la sécurité face à cette menace dans Office 2016.

SONICWALL®

Pourquoi les méthodes de prévention classiques ne marchent pas

Les contrôles de sécurité classiques échouent souvent à déceler un ransomware, parce que beaucoup d'entre eux ne traquent que les comportements inhabituels et les indicateurs standard de danger. Une fois sur le système, le ransomware se comporte comme une application de sécurité et peut bloquer l'accès à d'autres systèmes ou programmes. En général, les fichiers et systèmes concernés ne sont pas affectés, seul l'accès à l'interface est restreint.

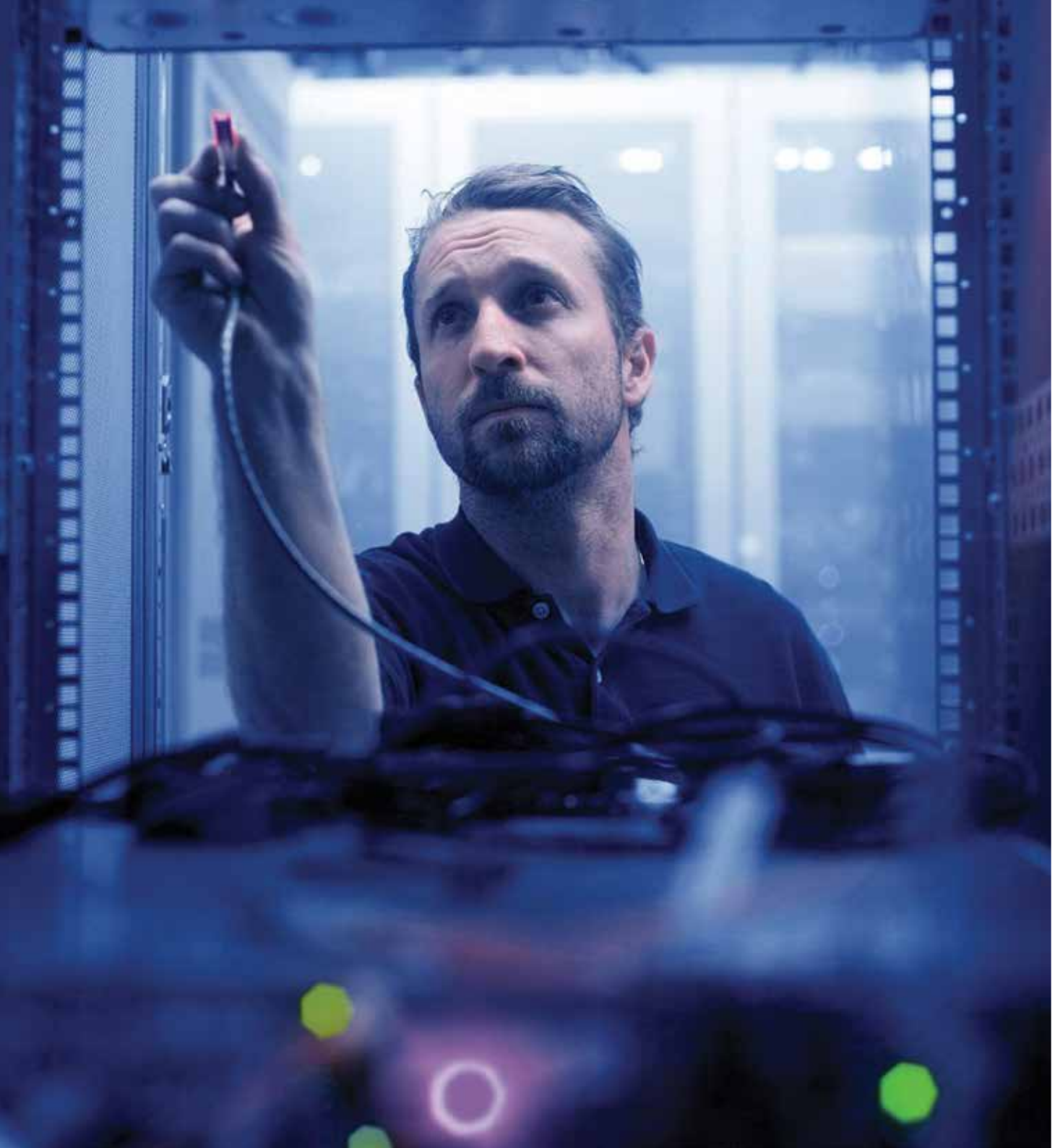
Les ransomwares alliés à l'ingénierie sociale peuvent produire une attaque très efficace.

Ransomwares cachés

Un ransomware peut aussi traverser inaperçu les pare-feux qui ne savent pas déchiffrer et inspecter le trafic SSL. En général, soit les solutions de sécurité réseau héritées sont incapables d'inspecter le trafic chiffré en SSL/TLS, soit leurs performances sont trop faibles pour pouvoir effectuer l'inspection. Or, il est de plus en plus fréquent que les cybercriminels cachent justement des malwares dans le trafic chiffré.

L'utilisation du chiffrement SSL (Secure Sockets Layer) ou TLS (Transport Layer Security) est en pleine explosion, avec pour conséquence une hausse des piratages non détectés, qui ont affecté au moins 900 millions d'utilisateurs en 2015.[3]

3 2016 SonicWall Annual Threat Report



Conclusion

SonicWall peut améliorer la protection de l'ensemble de votre structure en inspectant chaque paquet et en gouvernant chaque identité. Vos données sont protégées où qu'elles circulent, et le partage des renseignements sur la sécurité vous met à l'abri des menaces les plus diverses, dont les ransomwares.

Consultez la page Web des produits de sécurité réseau SonicWall.

SONICWALL®

À propos de nous

En 25 ans d'histoire, SonicWall a toujours été un partenaire industriel de confiance dans le domaine de la sécurité. De la sécurité réseau à celle des accès, en passant par la sécurisation de messagerie, SonicWall n'a cessé de développer son portefeuille de produits, permettant aux entreprises d'innover, d'aller plus vite et de croître. Avec plus d'un million d'appareils de sécurité en place dans près de 200 pays et territoires de par le monde, SonicWall permet à ses clients de dire en toute confiance oui à l'avenir.

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 plus d'informations sur les bureaux nationaux et internationaux.
www.sonicwall.com

Ebook-NS-Ransomware-EU-IMAG-29223 -D1

SONICWALL®