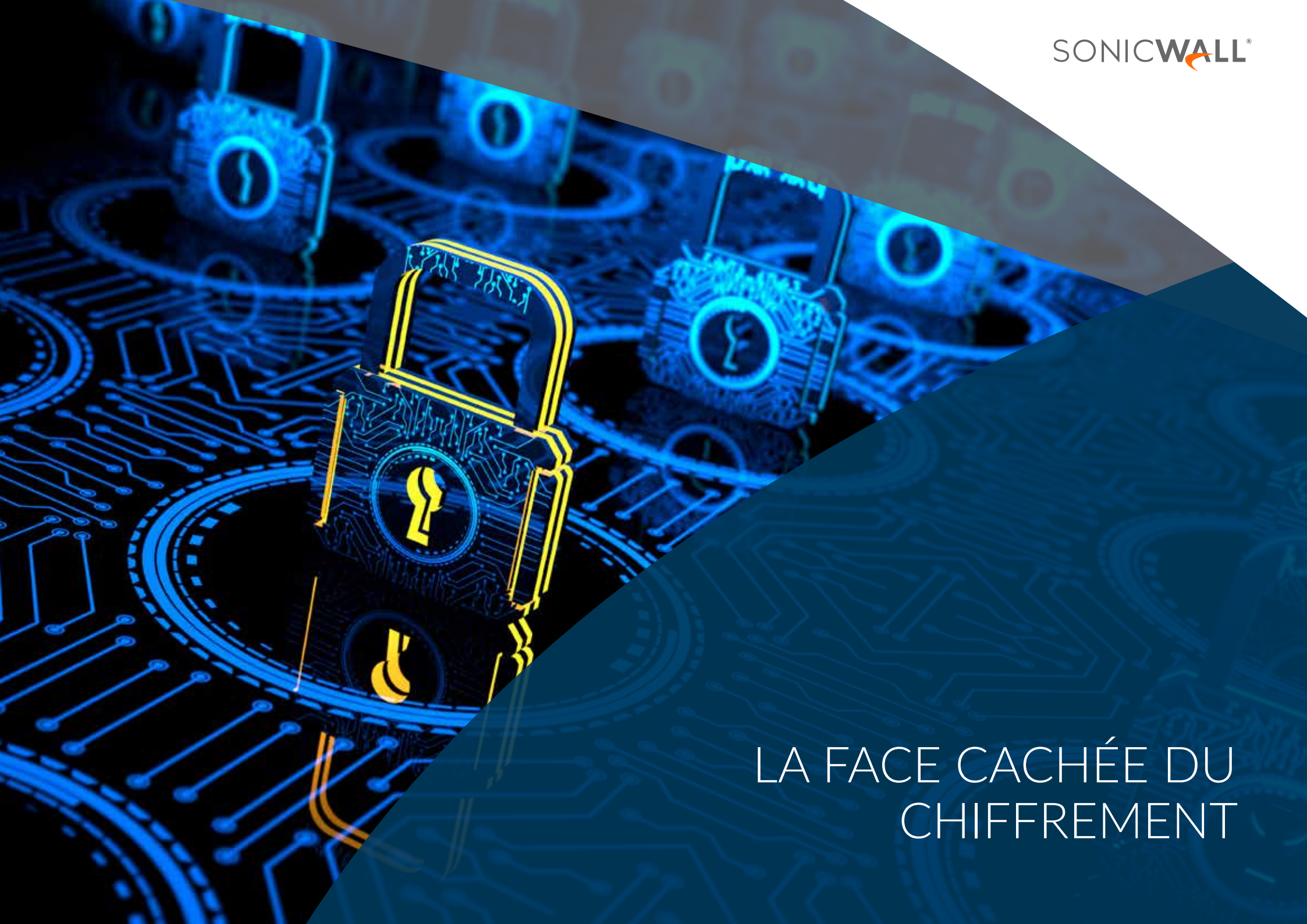
SONICWALL®



LA FACE CACHÉE DU CHIFFREMENT

Les hackers ont perfectionné leur art afin d'utiliser le trafic SSL dans le but de dissimuler leurs attaques et logiciels malveillants auprès des systèmes de sécurité.

97% des entreprises interrogées observent une augmentation du trafic Web chiffré.[1]

130% d'augmentation des menaces via les connexions TLS/SSL en 2016 par rapport à 2014.[1]

80% des entreprises interrogées ont été victimes d'une cyberattaque.[2]

41% des attaques étaient dissimulées dans le trafic SSL.[2]

[1] *Étude NSS Labs, juin 2016*
[2] *Étude Ponemon 2016*

SONICWALL®

Attaques exploitant le trafic SSL afin d'éviter toute détection

Attaque dissimulée dans le trafic « normal » port 443

- 78% des entreprises interrogées pensaient être susceptibles d'être visées.
- Moins d'un tiers (30%) des entreprises avaient confiance dans leur capacité à réagir.

Phishing

- 79% pensent qu'il est fort probable que cela puisse se produire dans leur entreprise.
- 17% seulement affirment que leur entreprise est en capacité de limiter ce type d'attaque.

Logiciels malveillants dissimulés dans les données sortantes du trafic chiffré

- 74% admettent que ce vecteur d'attaque est fort probable.
- 16% seulement indiquent que leur entreprise pourrait identifier et limiter l'attaque chiffrée avant exfiltration des données.

L'agresseur pourrait dissimuler les données sortantes et/ou dérobées sur un serveur de commande et contrôle.

- 66% déclarent que la probabilité d'un tel événement est fort possible.
- 26% pensent que leur entreprise pourrait détecter ce comportement et éviter la perte de données.

Étude Ponemon 2016

Comprendre l'utilisation malveillante du chiffrement

Demande de page : la machine de l'utilisateur (victime A) visite un bon site compromis.

Exécution du kit d'exploit : pendant que le contenu Web parvient au client, une petite partie du logiciel est téléchargée sur l'appareil de l'utilisateur, où une séquence de commande est exécutée pour exploiter les vulnérabilités logicielles sur l'ordinateur client.

Demande de logiciel malveillant : une fois que l'opérateur du kit d'exploit prend le contrôle de cet ordinateur, une commande est envoyée à un site Web qui héberge et fournit le logiciel malveillant.

Infection par le logiciel malveillant : le logiciel malveillant est installé chez la victime A.

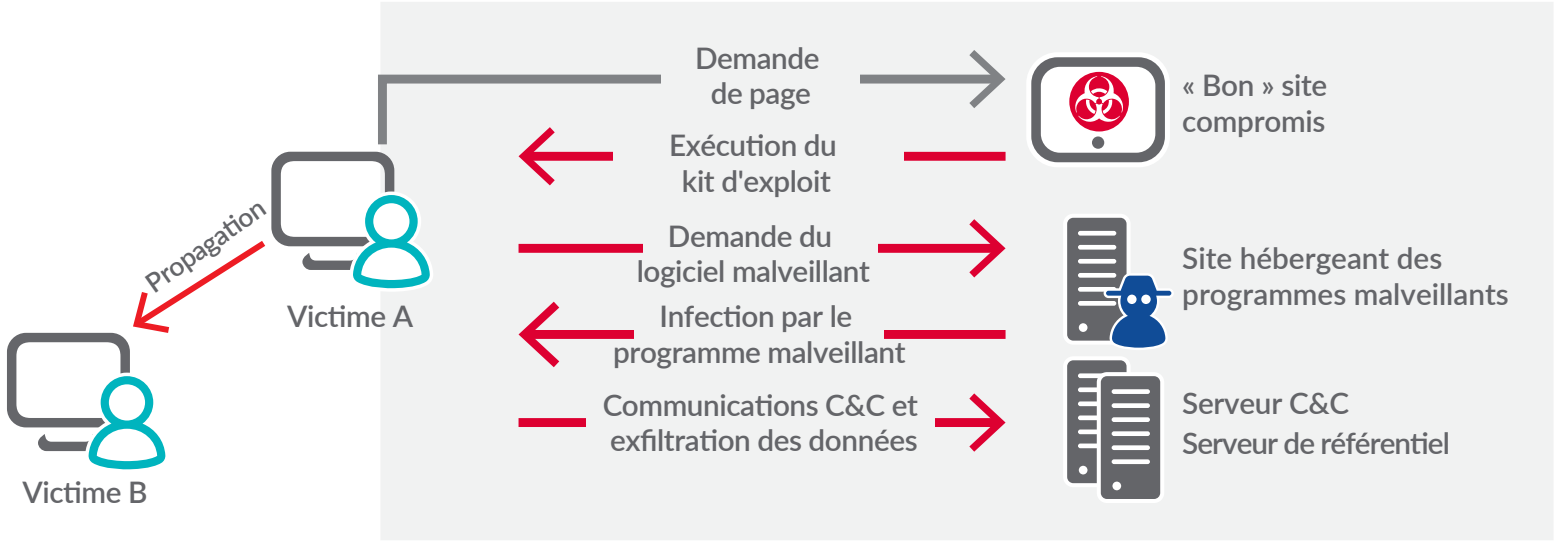
C&C : le logiciel malveillant communique à son tour avec une infrastructure de commande et contrôle afin d'obtenir davantage d'instructions.

Exfiltration de données : les données de la machine de la victime A sont copiées sur un serveur externe en vue d'être traitées.

Victime B : à ce stade, les agresseurs augmentent souvent leurs droits d'accès, ce qui leur permet de se déplacer de façon latérale au sein du réseau et d'infecter d'autres terminaux.

Chiffrement : en réalité, le chiffrement peut aujourd'hui être mis en place à n'importe quelle phase de cette attaque afin d'éviter toute détection.

Le chiffrement peut être mis en place à n'importe quelle phase d'une attaque



SONICWALL®

Trois obstacles courants à la non inspection du trafic SSL

Manque d'outils de sécurité

Ressources insuffisantes

Dégradation des performances

Source : Étude Ponemon 2016

SONICWALL®

L’impact sur les performances est un problème important.

- **61%** indiquent que le manque de performance est un problème pour les entreprises qui ne déchiffrent pas le trafic SSL.*

- **83%** déclarent que le déchiffrement entraîne une certaine dégradation dans les entreprises qui déchiffrent et analysent aujourd’hui le trafic SSL.*

**Source : Étude Ponemon 2016*

Poser les bonnes questions

- Savez-vous si le pare-feu de votre entreprise analyse le trafic HTTPS ?
- Votre entreprise a-t-elle subi de fréquentes interruptions de service du réseau ou des temps d'arrêt répétés suite à l'effondrement total des performances de votre pare-feu lors de l'analyse du trafic HTTPS ?
- Comment faites-vous évoluer la protection de votre réseau afin d'éviter la dégradation des performances, les retards et la latence de votre réseau lors de l'analyse du trafic HTTPS ?

Recommandations

- Si vous n'avez pas récemment réalisé d'audit de sécurité, il est judicieux de procéder maintenant à une évaluation complète de votre sécurité réseau afin d'identifier les risques et vos besoins.
- Mettez à jour vos règles de sécurité afin de vous protéger des menaces les plus diverses et instaurez plusieurs méthodes de défense pour faire face aux attaques, qu'il s'agisse de trafic HTTP ou HTTPS.
- Déployez un pare-feu de nouvelle génération avec fonctionnalité SSL/TLS (Secure Sockets Layer/Transport Layer Security) haute performance. Veillez à pouvoir analyser l'ensemble du trafic quels que soient les ports, les protocoles ou la taille des fichiers, en décompressant et en déchiffrant chaque paquet et en examinant chaque octet afin d'identifier rapidement les menaces.
- Les solutions standard de sandboxing ne détectent pas les logiciels malveillants dissimulés dans le trafic chiffré. L'inspection SSL/TLS est une nécessité, au même titre qu'une sandbox réseau qui bloque le trafic jusqu'à l'obtention d'un verdict et permet de détecter mais aussi d'éviter les attaques zero-day de manière automatisée.
- Ajoutez une fonctionnalité de filtrage de contenu pour empêcher les utilisateurs de visiter des sites douteux et utilisez un système d'antivirus et de prévention des intrusions au niveau de la passerelle pour les protéger des « bons » sites compromis.
- Rappelez régulièrement à vos équipes les dangers des médias sociaux, de l'ingénierie sociale, des sites Web et des téléchargements suspects, du spam et du phishing. Et surtout, dites à vos utilisateurs de ne jamais accepter des certificats auto-signés et non valables.
- Pratiquez une bonne cyberhygiène en veillant à bien actualiser vos logiciels avec toutes les mises à jour de sécurité. Cela protégera tous les ordinateurs contre d'anciens exploits SSL qui ont entre-temps été neutralisés.
- Établissez et répétez un plan de réponse et de correction. Testez régulièrement votre plan, effectuez des simulations de la même manière que pour un exercice d'évacuation incendie, améliorez le processus et veillez à ce que les premiers intervenants soient plus efficaces et mieux formés pour exécuter les plans de correction établis.

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 plus d'informations.
www.sonicwall.com