SONICWALL™

PRÉSENTATION : LA FACE CACHÉE DU CHIFFREMENT

Pourquoi votre solution de sécurité réseau doit être en mesure de déchiffrer le trafic pour stopper les menaces cachées

Résumé

Aujourd'hui, la plupart des sessions Web de vos utilisateurs sont vraisemblablement chiffrées à l'aide des protocoles de sécurisation SSL/TLS (Secure Sockets Layer/Transport Layer Security), ou HTTPS. De fait, dans le monde informatique, la tendance est au chiffrement de l'ensemble du trafic Internet, avec deux principaux objectifs :

- dissuader les cybercriminels d'espionner les connexions ;
- assurer la sécurité et la confidentialité des informations personnelles.

Une tendance dont les pirates ont eu tôt fait de s'accommoder, faisant des connexions chiffrées un vecteur privilégié pour masquer leurs attaques, contourner les systèmes de protection et, ainsi, se créer des portes dérobées au sein même des réseaux. Car vos contrôles de sécurité ne peuvent pas stopper ce qu'ils ne voient pas. Si aucune mesure n'est prise, les attaques exploitant SSL/TLS ont 100 % de chances d'aboutir, avec pour conséquence la perte de données confidentielles, de propriété intellectuelle et de votre réputation.

Le tout-chiffré

Les protocoles SSL/TLS sont couramment utilisés pour un peu tout, de l'e-commerce à la banque en ligne. Ils sécurisent un volume croissant de trafic dans les entreprises et représentent même la majeure partie du trafic réseau dans certains secteurs. SSL protège les données en mouvement en créant un canal chiffré par dessus le réseau Internet public ou les réseaux privés. De cette manière, les données ne peuvent être ni interceptées ni compromises.

De plus, SSL vérifie que les données ne sont pas envoyées vers un hacker usurpant une destination de confiance. Les données vitales et sensibles, telles que les informations de cartes de crédit, les noms d'utilisateur et les mots de passe, sont transportées de manière à ce que seul le destinataire y ait accès. À l'origine, les sites Web et les serveurs FTP ou Telnet étaient les principaux utilisateurs de SSL. Mais aujourd'hui, les applications sont nombreuses à utiliser ce protocole, notamment les applications Java, les services de gestion des applications et les services cloud. Facebook et Twitter sont également deux des applications les plus répandues fonctionnant avec SSL. Il existe en outre

En général, soit les solutions de sécurité réseau en place sont incapables d'inspecter le trafic chiffré en SSL/TLS, soit leurs performances sont trop faibles pour pouvoir effectuer l'inspection.

des extensions de navigateur capables d'imposer l'utilisation de SSL via HTTPS.[1]

Au quatrième trimestre 2015, les connexions HTTPS (SSL/TLS) comptaient en moyenne pour 64,6 % des connexions Web, soit une croissance supérieure à HTTP sur la majeure partie de l'année. En janvier 2015, les connexions HTTPS ont augmenté de 109 % par rapport à janvier 2014. Et sur chaque mois de 2015, une augmentation moyenne de 53 % a été enregistrée par rapport au mois correspondant de 2014.

L'analyse du trafic chiffré, un défi pour les pare-feux

Doués, les assaillants peuvent créer des communications C&C et du code malveillant avec SSL/TLS pour échapper aux systèmes de prévention des intrusions (IPS) et de filtrage anti-malware. Ces attaques peuvent être extrêmement efficaces, tout simplement parce que la plupart des entreprises n'ont pas l'infrastructure adéquate pour les détecter. En général, soit les solutions de sécurité réseau en place sont incapables d'inspecter le trafic chiffré en SSL/TLS, soit leurs performances sont trop faibles pour pouvoir effectuer l'inspection. Le filtrage du trafic HTTPS par un pare-feu nouvelle génération nécessite six traitements de plus que le filtrage du trafic en clair.

Les deux processus qui affectent le plus les performances sont :

- l'établissement d'une connexion sécurisée ;
- le déchiffrement et le re-chiffrement du trafic pour l'échange sécurisé des données.

Le poids sur les performances peut parfois être lourd, rendant le filtrage SSL/TLS quasi prohibitif pour les entreprises équipées d'anciens systèmes de sécurité.

La plupart des cyberattaques ont un caractère opportuniste et des motivations financières. Autrement dit, toute organisation est susceptible d'en être la cible.

Les risques pour votre entreprise

Tout au long de l'année, les assaillants ont pleinement profité de l'augmentation du trafic HTTPS et du manque de visibilité. À l'exemple de cette attaque perpétrée via une publicité sur Yahoo, qui a exposé pas moins de 900 millions d'utilisateurs à un programme malveillant. La campagne en question redirigeait les visiteurs de Yahoo vers un site infecté par Angler Exploit Kit. 10 millions d'autres utilisateurs ont probablement été affectés durant les semaines précédentes en accédant à des publicités placées par une société de marketing appelée « E-planning ».

Conclusion

Le chiffrement est omniprésent, ce qui en fait un vecteur de menaces privilégié pour les pirates. Votre solution de sécurité réseau doit savoir déchiffrer le trafic pour stopper les menaces cachées.

Pour en savoir plus, lisez notre document « Meilleures pratiques pour stopper les menaces chiffrées. »

[1] *UBM Tech E-paper: Next-Gen Security*

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

SolutionBrief-DarkSideOfEncryption-EU-IMAG-22649