SONICWALL

DOSSIER : COMPRENDRE LES MENACES CHIFFRÉES

Comment les cybercriminels dissimulent leurs attaques sur votre réseau via SSL/TLS

Résumé

Les technologies de chiffrement SSL/TLS et HTTPS offrent une protection contre le piratage et leur utilisation connaît une croissance exponentielle. Mais les cybercriminels ont appris à exploiter l'efficacité du chiffrement pour dissimuler leurs logiciels malveillants, ransomwares, attaques de spear-phishing, zero-day, exfiltration de données, sites malveillants et autres attaques. Il existe heureusement des solutions de sécurité réseau avancée avec inspection approfondie des paquets du trafic SSL/TLS et HTTPS qui protègent des menaces chiffrées.

Les types de menaces chiffrées

Si le chiffrement offre une protection pour le trafic légitime, il peut aussi servir de support pour dissimuler des cyberattaques. Autrement dit, le protocole SSL (Secure Sockets Layer) peut créer un tunnel chiffré pour sécuriser les données via un VPN. Le protocole TLS (Transport Layer Security) est une version actualisée et plus sécurisée du SSL. Le protocole HTTPS (Hyper Text Transfer Protocol Secure) apparaît dans l'URL lorsqu'un site Web est sécurisé par un certificat SSL.

Il existe plusieurs catégories de menaces chiffrées. L'une de ces catégories correspond aux menaces liées aux vulnérabilités des certificats. Dans ce cas, lorsque vous communiquez avec un site, votre navigateur ou une application peuvent afficher une alerte signalant que la connexion est non sécurisée ou non fiable. La certification n'est pas efficace dans ce type de situation. L'autorité de certification est peut-être injoignable ou le certificat n'est pas valide. Ou bien le chiffrement n'est pas souhaitable, qu'il s'agisse d'une forme plus ancienne de SSL (qui, à ce stade, n'est plus utilisé), d'une forme inférieure de TLS ou de signatures et de méthodes de hachage qui ne correspondent pas à ce qu'elles devraient être selon les normes actuelles de chiffrement.

Une autre catégorie de menaces chiffrées inclut les logiciels malveillants qui incorporent toutes ses communications dans un tunnel chiffré de manière à contourner la sécurité de votre réseau. Parmi les applications qui obscurcissent volontairement leur trafic et leurs communications, on peut citer Psiphon, Tor et Ultrasurf.

Puis il y a les failles réelles dans le trafic chiffré, les logiciels malveillants qui dérobent les identifiants, tels que DROWN, Heartbleed, PODDLE et FREAK. Il existe des exploits qui profitent du chiffrement lui-même pour jouer l'homme du milieu et intercepter vos e-mails, identifiants, informations personnelles, données de transactions en ligne, etc. Si ce type d'attaque a compromis votre réseau, il peut ultérieurement l'utiliser contre vous ou incorporer la menace au sein même des communications, pour vous envoyer vers des sites Web tiers ou injecter des applications malveillantes dans les connexions de votre navigateur.

Historique des menaces chiffrées

Pour comprendre les conditions permettant de se protéger de ces menaces, il convient d'en connaître l'historique. L'ancien modèle de sécurité des pare-feux des années 1990 et du début des années 2000 repose sur la technologie SPI (inspection stateful des paquets). En fait, des millions de pare-feux dotés uniquement de la technologie SPI sont encore aujourd'hui utilisés sur Internet.

Cette technologie peut être comparée au rôle d'un agent de la circulation qui arrête ou relance le trafic à un carrefour. L'agent peut uniquement voir les informations extérieures aux véhicules, comme la marque et le modèle, la plaque d'immatriculation et la direction dans laquelle ils se dirigent, mais ne voient rien de ce qui est caché sur la banquette arrière, sous le capot ni dans le coffre. Si l'un d'eux recèle quelque chose d'illicite, il ne peut donc pas le voir.

À l'inverse, l'inspection approfondie des paquets (DPI), que laquelle reposent les pare-feux de nouvelle génération, permet à ces derniers de procéder à une inspection au niveau de la couche 7. C'est comme si notre agent de la circulation était doué d'une vision au rayon-x pour voir les recoins cachés des véhicules, puis décider quelle file de voitures était autorisée à traverser ou non le carrefour.

> Internet devient rapidement un modèle complètement chiffré.

Cette vision au rayon-x ne lui permet toutefois pas de voir au travers du plomb (selon notre analogie, le protocole HTTPS). Pour surmonter cet obstacle, la technologie DPI doit inclure la possibilité d'inspecter le trafic SSL chiffré (DPI-SSL).

La croissance explosive du trafic HTTPS chiffré

Conséquence de l'effet « Snowden », l'affaire d'espionnage de la NSA, ou tout simplement efforts louables pour empêcher de potentiels agresseurs et pirates de violer votre vie privée en ligne, un volume considérable du trafic Internet actuel est désormais chiffré via HTTPS.

Une connexion HTTPS est essentiellement une connexion sécurisée ou privée, établie depuis l'application de départ (habituellement un navigateur), qui parcourt l'ensemble du réseau et Internet vers le serveur ou le site de destination. Ces connexions HTTPS incluent webcasts, recherches en ligne, applications de productivité Cloud, messagerie Web, etc. Le protocole HTTPS est essentiellement un VPN. C'est une connexion Web chiffrée établie depuis votre navigateur vers la destination. Et comme c'est un VPN, vous ne pouvez pas voir à l'intérieur. Il n'est pas possible d'inspecter le trafic traversant la connexion HTTPS ni de déterminer si des logiciels malveillants cherchent à y entrer ou si des données sensibles s'échappent de votre réseau.

Internet devient rapidement un modèle complètement chiffré. Les nouvelles tendances sont au « tout chiffré » et même les principaux moteurs de recherche ont modifié leurs algorithmes de recherche pour hiérarchiser les sites HTTPS dans leurs résultats de recherche. Prenons par exemple un distributeur en ligne qui bénéficie par mois de dizaines de milliers de clics supplémentaires par rapport à un concurrent, mais qui n'utilise pas l'HTTPS sur sa page de destination. Les résultats de recherche le placeront après son concurrent, pourtant moins performant, mais qui lui utilise l'HTTPS sur sa page de destination.

Plus de la moitié des applications Web utilisent désormais l'HTTPS. Les grandes applications comme Office 365, YouTube, Amazon, SAP, Salesforce, Skype, Dropbox, Twitter et Gmail utilisent toutes le chiffrement. Les grands analystes prédisent que 65 pour cent du trafic Internet mondial sera chiffré d'ici l'année prochaine. Autrement dit, pour une connexion Internet de 100 Mbit/s, environ 65 Mbit/s de ce trafic échapperont à toute inspection. Sur une heure, cela représente environ 4 à 7 DVD de données transférées sans être inspectées. Sur certains réseaux, la quantité totale de données personnelles confidentielles et de propriété intellectuelle peut même représenter un volume inférieur. Réfléchissez à l'impact éventuel si vous ne pouviez pas voir ce volume de données entrer ou sortir de votre réseau.

Et nous parlons ici uniquement du trafic Internet habituel. En moyenne, l'HTTPS est mis en place dans 60 à 80 pour cent des entreprises, selon le secteur d'activité. Par exemple, dans le domaine financier, bancaire ou de la santé, la plupart de vos sites sont déjà chiffrés.

Une utilisation criminelle du chiffrement

Alors que le trafic chiffré a permis de renforcer la sécurité dans nos communications quotidiennes, les cybercriminels profitent de la confidentialité possible avec l'HTTPS pour dissimuler leurs attaques. Ils ont appris à manipuler le chiffrement pour échapper à la plupart des anciennes solutions de pare-feux. Par conséquent, la majorité du trafic HTTPS actuel n'est pas inspecté, même par des pare-feux récents. Votre trafic étant pour l'essentiel invisible à votre pare-feu, la question n'est pas de savoir si une inspection a lieu ni même quand elle a lieu. Votre réseau est probablement déjà compromis.

Les grands titres des journaux nous apprennent que Yahoo, IRS et Ashley Madison ont tous subi des brèches liées au chiffrement. Dans un cas, ce sont plus d'un milliard de comptes de messagerie qui ont été compromis suite à l'envoi d'un seul message chiffré de spear-

phishing à un seul employé. De même, la brèche OPM (dans laquelle plus de 20 millions d'utilisateurs ont subi une fuite en ligne de leurs informations top secrètes d'autorisation) a été causée par le téléchargement d'un seul e-mail personnel, qui n'a pas été inspecté et qui contenait un logiciel malveillant. Le trafic chiffré peut contenir des logiciels malveillants, des données confidentielles provenant d'une fuite accidentelle ou volontaire ou véhiculer une attaque de spear-phishing contre le département financier en vue de recevoir un règlement par virement bancaire. Voici quelques exemples de menaces dissimulées dans le trafic chiffré.

Logiciels malveillants exploitant la messagerie chiffrée

Comment empêcher un utilisateur de cliquer sur une pièce jointe qui déclenche un logiciel malveillant sur votre réseau ? S'il s'agit d'un malware comme Cryptolocker, il contient une charge utile malveillante téléchargée dans la messagerie Web ou toute autre communication chiffrée. Si elle est chiffrée, il n'est pas possible de l'inspecter, de la contrôler ni de la bloquer. Pour bloquer les e-mails, leurs pièces jointes ou les liens sur lesquels l'utilisateur clique, il faut pouvoir capturer le trafic chiffré, le déchiffrer et en inspecter le contenu.

Ransomwares chiffrés

Le type de logiciels malveillants chiffrés les plus répandus sont les ransomwares (notamment WannaCry, CryptoLocker, Zeus, Chimera et Tesla). Les ransomwares utilisent le chiffrement de plusieurs façons. Tout d'abord, la livraison effective des ransomwares via une communication chiffrée, qu'il s'agisse de messagerie Web, de sites de réseaux sociaux, d'applications de messagerie instantanée ou de messages texte. Une fois livré via une communication chiffrée, le ransomware s'exécute souvent puis appelle son serveur de commande et contrôle (C&C) par le biais d'une autre communication chiffrée. Ce n'est donc pas seulement le message contenant la charge utile qui est chiffré mais également la communication qui revient vers le serveur C&C.

Spear-phishing chiffré

Dans une attaque type de spear-phishing, l'utilisateur s'identifie dans sa messagerie Web chiffrée, ouvre un e-mail de spear-phishing qui semble provenir d'un collègue connu, clique sur un lien HTTPS et exécute un fichier téléchargé. Les données de son ordinateur sont alors instantanément chiffrées et ne sont plus disponibles. Une fenêtre demande le paiement d'une rançon pour pouvoir accéder au fichier.

Selon l'US-CERT, plus de 5 milliards de dollars ont été détournés dans des entreprises l'année passée, par le biais de virements bancaires résultant d'attaques de spear-phishing et de whaling. Le FBI estime que ces pertes représentent plus de 1000 milliards depuis 2014. La société FACC a été victime d'un détournement de 54 millions de dollars en une seule attaque de spear-phishing. Et ce type d'attaques continue de se produire tous les jours.

Sites Web malveillants chiffrés

Le simple fait d'être chiffré via HTTPS ne garantit pas pour autant qu'un site est protégé. De nombreux sites chiffrés sont malveillants et contiennent des menaces zero-day dont les signatures ne sont pas connues des pare-feux. Sans ces signatures, le pare-feu ne saura pas toujours reconnaître le logiciel malveillant correspondant sur le site. En mai 2018, l'US-CERT a signalé plus de 300 nouveaux cas de vulnérabilités répertoriées au CVE (Common Vulnerabilities and Exposures). Présentes dans le système d'exploitation Google Android, il s'agissait de 59 vulnérabilités de niveau critique.

Attaques zero-day chiffrées

Même si votre réseau est protégé par une solution antivirus très efficace, vous ne pourrez pas toujours avoir les signatures à temps pour contrer les exploits zero-day. Un logiciel malveillant de type zero-day est un code écrit peut-être quelques instants avant l'attaque, et qui est donc encore inconnu ; aucun pare-feu ne possède la signature correspondante et ne peut donc le bloquer. Les logiciels malveillants peuvent en effet pénétrer sur le réseau et désactiver l'antivirus client. Les premières lignes de code du virus sont conçues pour désactiver la solution antivirus ; le logiciel malveillant est alors déclenché. L'US-CERT a récemment indiqué que même l'antivirus intégré dans Microsoft Defender a été compromis pour permettre son exploitation depuis l'extérieur.

> Toutes les plus grandes brèches médiatisées au cours des cinq dernières années visaient le chiffrement ou étaient liées à une charge utile chiffrée.

Conclusion

Il existe heureusement des solutions pour lutter contre l'exploitation malveillante de l'HTTPS, tout en conservant la possibilité de chiffrer le trafic afin que les pirates ne puissent pas y accéder. Vous pourrez en savoir plus sur les solutions SonicWall complètes et avancées contre les menaces chiffrées dans notre fiche technique Déchiffrement et inspection du trafic chiffré.

[1] https://www.wsj.com/articles/yahoo-discloses-new-breach-of-1-billion-user-accounts-1481753131
[2] https://www.wsj.com/articles/opm-breach-exposed-19-7-million-background-clearance-forms-1436469626
[3] http://www.securityweek.com/cybercriminals-steal-54-million-aircraft-parts-maker

À propos de nous

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.
1033 McCarthy Boulevard
Milpitas, CA 95035

Consultez notre site Internet pour plus d'informations.
www.sonicwall.com

SolutionBrief-UnderstandingEncryptedThreats-US-KJ-MKTG2859

SONICWALL®