ÉTAT DES LIEUX D'INTERNET ÉTÉ 2018

[État des lieux d'Internet] / Sécurité

PRÉSENTATION

Présentation

Akamai, plateforme de diffusion dans le cloud la plus fiable et la plus utilisée au monde, s'appuie sur sa solution Akamai Intelligent Platform™ distribuée mondialement, pour traiter plusieurs milliards de transactions sur Internet chaque jour. Cette plateforme nous permet de recueillir de grands volumes de données sur divers indicateurs, tels que la connectivité haut débit, la sécurité dans le cloud et la diffusion de contenu multimédia. Chaque trimestre, Akamai publie ses rapports *État des lieux d'Internet* à partir de ces données, en mettant l'accent sur la connectivité haut débit et la sécurité dans le cloud.

RÉPERCUSSIONS COMMERCIALES

Les attaques de ces derniers mois nous rappellent que l'état des lieux de la sécurité sur Internet n'est pas statique. Les attaquants font preuve d'une ingéniosité sans cesse renouvelée pour découvrir de nouveaux vecteurs, exploiter de nouvelles vulnérabilités et développer des stratégies d'attaque plus perturbatrices que jamais. En 2017, de nouvelles catégories de terminaux (téléphones portables et terminaux IoT en particulier) ont été utilisées pour créer de vastes botnets responsables d'attaques d'une taille record. Néanmoins, au cours des deux premiers mois de 2018, ces records ont été d'emblée battus lorsque des pirates ont exploité un nouveau vecteur, Memcached (un service qui n'était à la base pas conçu pour être exposé à Internet), pour générer des attaques massives d'une taille supérieure à 1 Tbit/s. Avec Memcached, ces attaques prennent une ampleur inédite pour des attaques par réflexion.

Heureusement, dans ce cas précis, une réponse rapide des développeurs, des opérateurs réseau et des fournisseurs de services semble avoir considérablement réduit le nombre de serveurs Memcached vulnérables, ce qui devrait à l'avenir limiter le potentiel de ce nouveau vecteur d'attaque. Cette piqûre de rappel vient à point pour alerter la communauté sur les dangers de la complaisance : nous ne devons jamais baisser la garde face aux tendances et aux avancées technologiques et nous tenir prêts à faire face à des attaques de taille croissante. Par ailleurs, la communauté tout entière doit suivre de près et actualiser les correctifs logiciels et les configurations sécurisées pour minimiser l'accès des cybercriminels aux surfaces d'attaque.

PRÉSENTATION DE L'ÉDITEUR

Ce rapport évolue de concert avec l'évolution de l'état des lieux de la sécurité sur Internet. Nous allons modifier sa fréquence de publication, son format et sa structure afin de vous communiquer nos données et les résultats de nos recherches d'une manière aussi rapide et pertinente que possible. Les données statistiques et les graphiques illustrant les attaques DDoS ou visant les applications Web (y compris les graphiques relatifs à la taille des attaques et à la fréquence des vecteurs DDoS) se trouvent désormais pour la plupart sur notre site Web. Pour ne manquer aucune mise à jour, consultez notre blog. Par ailleurs, nous publierons régulièrement des rapports simplifiés axés sur les tendances à long terme, les recherches et les analyses. Le rapport *État des lieux d'Internet / Sécurité : attaques Web* sera désormais publié deux fois par an, en hiver et en été.

Notre Analyse d'une attaque à l'été 2018 se concentre sur l'attaque par réflexion Memcached de février 2018, qui est à ce jour la plus importante attaque contrée par Akamai. Avec 1,3 Tbit/s, elle représente plus de deux fois la taille du précédent record (623 Gbit/s) détenu par Mirai depuis septembre 2016. Les attaques DDoS

1 Tbit/s

Palier franchi par le réflecteur Memcached

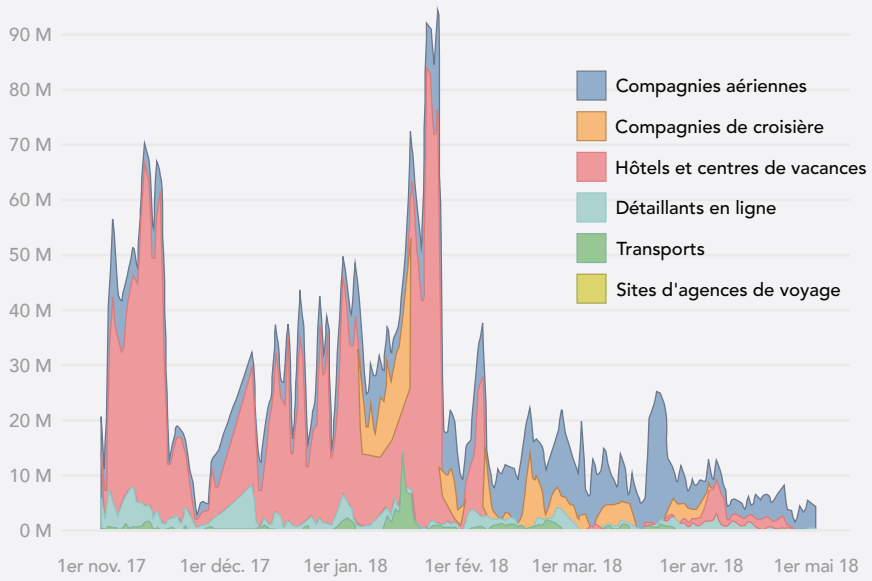
de taille moyenne atteignent désormais régulièrement 1,3 Gbit/s et leur nombre ne cesse d'augmenter, c'est pourquoi il est indispensable que toutes les organisations se préparent à faire face à des attaques à grande échelle.

Dans notre rapport *État des lieux d'Internet à l'été 2018 / Sécurité : attaques Web*, nous examinons plusieurs attaques DDoS utilisant des tactiques inhabituelles pour gagner en efficacité. Alors que la majorité des attaques DDoS sont de nature simple et volumétrique, quelques-unes d'entre elles montrent les signes d'un ennemi intelligent et évolutif, capable d'adapter sa tactique pour surmonter les défenses qui lui barrent la route.

L'initiative « Operation Power Off », visant à fermer les sites DDoS-for-hire, est un sujet particulièrement intéressant. En avril 2018, un effort coordonné des autorités policières de plusieurs pays a ainsi permis de fermer le site Webstresser.org, acteur majeur sur le marché DDoS-for-hire et responsable présumé de millions d'attaques. Néanmoins, ces sites sont remarquablement lucratifs et il ne serait pas surprenant d'en voir de nouveaux envahir la toile dans un avenir proche.

Enfin, sur la base des données relatives aux bots et au vol d'identifiants analysées dans notre rapport *État des lieux d'Internet / Sécurité au 4e trimestre 2017*, nous avons approfondi le sujet afin de mieux caractériser et comprendre à la fois les bots et les voleurs d'identifiants dans le secteur hôtelier, victime à ce jour du plus grand pourcentage de connexions malveillantes. Nous observons également que la fermeture de plusieurs itinéraires en février 2018 semble avoir entraîné un net déclin du trafic malveillant.

fig 1.1 **Tentatives de connexions malveillantes : hôtellerie et tourisme**



ATTAQUES DDOS, COMPARATIF ÉTÉ 2017 / ÉTÉ 2018

16 % d'attaques DDoS supplémentaires

16 % d'attaques d'infrastructure (couches 3 et 4) supplémentaires

4 % d'attaques par réflexion supplémentaires

38 % d'attaques de couche applicative supplémentaires

Pour consulter d'autres analyses et études, téléchargez le rapport complet.

Le rapport *État des lieux d'Internet à l'été 2018 / Sécurité : attaques Web* réunit les données d'attaques de l'infrastructure mondiale d'Akamai et présente les recherches de nombreuses équipes de l'entreprise.

ÉTAT DES LIEUX D'INTERNET / ÉQUIPE DE SÉCURITÉ

Jose Arteaga, Akamai SIRT, Data Wrangler — Attack Spotlight
Dave Lewis, Global Security Advocate — Operation Power Off
Wilber Mejia, Akamai SIRT — Attack Spotlight
Elad Shuster, Security Data Analyst Advanced DDoS — Akamai Blog
David McEwan, Security Operations Command Center — Advanced DDoS
Alejandro Ziegenhirt, Security Operations Command Center — Advanced DDoS

ÉQUIPE ÉDITORIALE

Martin McKeay, Senior Security Advocate, Senior Editor
Amanda Fakhreddine, Sr. Technical Writer, Editor

CRÉATION

Shawn Broderick et Sajeesh Alakkaparambil, Design
Georgina Morales Hampe et Kylee McRae, Project Management

À PROPOS D'AKAMAI

En proposant la plate-forme de diffusion cloud la plus étendue et la plus fiable au monde, Akamai aide ses clients à fournir les expériences numériques les plus efficaces et sécurisées, partout, à tout moment et sur tous les terminaux. La plateforme massivement distribuée d'Akamai bénéficie d'un déploiement inégalé avec plus de 200 000 serveurs dans 130 pays, offrant ainsi aux clients des niveaux avancés de performances et de protection contre les menaces. Les solutions d'Akamai, dédiées à l'optimisation des performances sur le Web et sur mobile, à l'accès professionnel, à la sécurité dans le cloud et à la diffusion de vidéos, sont renforcées par un service client exceptionnel et une surveillance 24 h/24, 7 j/7. Pour découvrir pourquoi de grandes institutions financières, des leaders du e-commerce, des entreprises du divertissement et des médias ainsi que des organisations gouvernementales font confiance à Akamai, consultez les sites https://www.akamai.com/fr/fr/, blogs.akamai.com ou suivez @Akamai sur Twitter. Vous trouverez nos coordonnées dans le monde entier à l'adresse www.akamai.com/locations. Vous pouvez également nous contacter au +33-185644654. Publication : 06/18.