[État des lieux d'Internet] / Sécurité

Présentation du 4e trimestre 2017

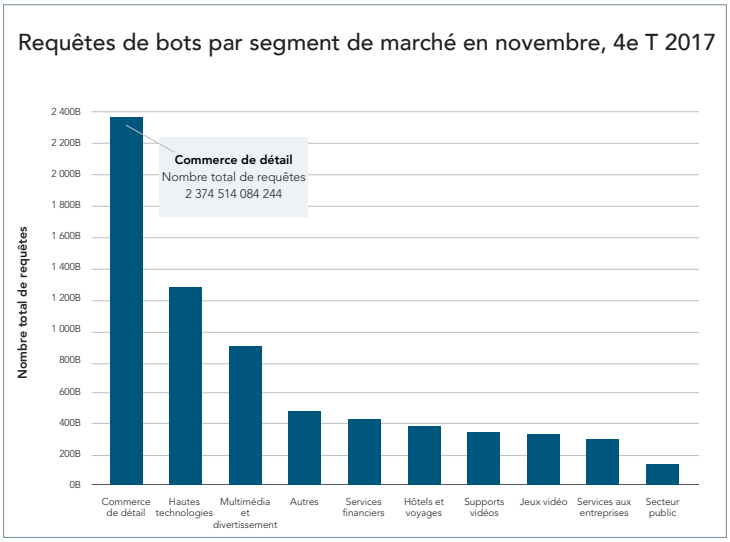
Akamai

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 plate-forme 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. Le rapport *État des lieux d'Internet* a été créé pour permettre aux entreprises et aux gouvernements de prendre des décisions stratégiques et éclairées en exploitant ces données et les connaissances qu'il fournit. 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.

Conséquences commerciales / Avec certaines des attaques les plus coûteuses et perturbatrices à ce jour, les incidents majeurs de l'année 2017 ont accéléré la prise de conscience de la nature stratégique de la cybersécurité. Les dangereuses failles matérielles qui ont activé Spectre et Meltdown ont permis à des programmes malveillants de lire les données en mémoire d'un ordinateur sans les privilèges requis. L'existence de telles vulnérabilités insidieuses et omniprésentes, avec les répercussions désastreuses qu'elles peuvent avoir, devrait suffire à éveiller l'attention même des plus optimistes.

De nombreuses attaques actuelles continuent d'exploiter des vulnérabilités bien connues ; des failles qui ont été documentées et corrigées, et qui peuvent être évitées. Même si cela est sûrement plus facile à dire qu'à faire, des efforts collectifs visant à couvrir les considérations de base - pratiques de codage sécurisées, correctifs en temps opportun, configuration correcte des périphériques et gestion prudente des mots de passe - contribueraient grandement à fortifier les défenses.

Le paysage de la sécurité est en constante évolution, car les cybercriminels tirent profit des nouvelles surfaces d'attaque. Les attaques ciblant les appareils mobiles, l'Internet des objets et les API sont au centre de nos préoccupations pour 2018. Les stratégies de cyberattaque continuent d'évoluer. Nous observons une nouvelle tendance qui consiste à cibler les systèmes d'entreprise, non seulement pour leur voler leurs données, mais également leurs ressources informatiques, peut-être motivée en partie par le développement des crypto-monnaies et de la valeur potentielle du minage de ressources. En outre, ce trimestre, le rapport *État des lieux d'Internet / Sécurité* examine certains ensembles de données uniques sur la connectivité réseau d'Akamai, le trafic des botnets et les vols d'identifiants, révélant qu'un pourcentage élevé (43 %) de tentatives de connexion sur les sites Web sont malveillantes. Une bonne compréhension de ces tendances est désormais essentielle au bien-être de toute entreprise connectée en numérique.



Présentation de l'éditeur / À l'aube de cette nouvelle année, le moment est bien choisi pour réfléchir sur les enseignements de la précédente.

D'une année sur l'autre, les chiffres indiquent que les attaques DDoS et d'applications Web ne cessent d'augmenter, les criminels continuant à faire bon usage de vecteurs d'attaque connus et éprouvés. Cela illustre l'incontestable importance de l'adoption de meilleures pratiques de sécurité élémentaires, par exemple la configuration et l'application de correctifs aux périphériques connectés, ainsi que le respect de règles de codage sécurisées telles que le nettoyage des données saisies.

Au 4e trimestre, nous avons constaté l'impact et l'évolution du botnet Mirai. Le rapport *État des lieux d'Internet / Sécurité* de ce trimestre s'intéresse à l'activité et l'évolution de Mirai au cours de la dernière année afin de nous préparer à ce l'avenir nous réserve. Larry Cashdollar, membre de l'équipe SIRT d'Akamai, examine en détail quelques-unes des vulnérabilités dont vous devez être informé. Les vulnérabilités analysées comptent parmi les plus graves, car elles permettent une exécution sur un système sans nécessiter d'authentification. Nous avons également eu l'occasion d'examiner ce trimestre deux ensembles de données de données qui n'ont pas encore figuré dans le rapport *État des lieux d'Internet / Sécurité* : l'analyse du trafic des bots et l'analyse des tentatives de vol d'identifiants.

ATTAQUES DDoS [comparatif 4e T 2017/3e T 2017]

- Baisse de moins de 1 % du nombre total d'attaques DDoS
- Baisse de 1 % du nombre d'attaques d'infrastructure (couches 3 et 4)
- Baisse de 3 % du nombre d'attaques par réflexion
- Augmentation de 115 % des attaques de couche applicative

Enfin, nous pensons que les crypto-devises se tailleront la part du lion dans l'actualité des cyberattaques en 2018. Dans cette tendance que nous percevons, il est possible que des machines d'entreprise soient infiltrées pour leurs ressources informatiques, et les crypto-devises constituent une force susceptible d'orienter de bien d'autres façons les stratégies en constante évolution des hackers.

Mise à jour sur les attaques DDoS / Les attaques par déni de service distribué (DDoS) peuvent provoquer l'arrêt de sites Web, perturber des activités et détourner des ressources, tout en servant parfois de couverture pour des violations de données ou de systèmes plus insidieuses. Après deux trimestres d'attaques croissantes, au cours du quatrième trimestre de 2017, les attaques DDoS se sont stabilisées, diminuant très légèrement (moins de 1 %) par rapport au trimestre précédent. Les attaques de la couche applicative ont notamment augmenté de manière significative de 115 % d'un trimestre à l'autre, mais elles représentent encore moins de 1 % de l'ensemble des attaques DDoS. Les attaques DDoS ont connu une augmentation de 14 % par rapport au 4e trimestre 2016, indiquant une tendance globale à la hausse à plus long terme.

Le secteur du jeu a été le plus ciblé, subissant 79 % de l'ensemble des attaques DDoS au 4e trimestre. Le deuxième secteur le plus attaqué, les services financiers, a connu une forte progression de l'activité DDoS au quatrième trimestre, avec un record de 45 attaques en une seule semaine. La fréquence de ces attaques souligne la nécessité d'une solution de protection contre les attaques DDoS fiable, non seulement pour prévenir les perturbations, mais aussi pour se protéger contre les attaques polymorphes qui peuvent utiliser des campagnes DDoS comme couverture pour des tentatives de violation de systèmes plus insidieuses.

Mise à jour sur les attaques d'applications Web / Contrairement aux attaques DDoS, les attaques d'applications Web ciblent habituellement les vulnérabilités des applications dans le but de voler des données ou de compromettre le système sous-jacent. Les attaques d'applications Web sont bien plus répandues que les attaques DDoS, les attaquants se contentant bien souvent de rechercher sur Internet les sites les plus vulnérables. Suite à une hausse considérable de 30 % au 3e trimestre, les attaques d'applications Web ont connu une légère diminution au 4e trimestre, mais elles ont tout de même augmenté significativement en 2017, une tendance qui, selon nous, devrait se poursuivre en 2018.

ATTAQUES D'APPLICATIONS WEB [comparatif 4e T 2017/3e T 2017]

- Diminution de 9 % du nombre total d'attaques d'applications Web
- Diminution de 29 % des attaques originaires des États-Unis
- Augmentation de 9 % du nombre d'attaques SQLi

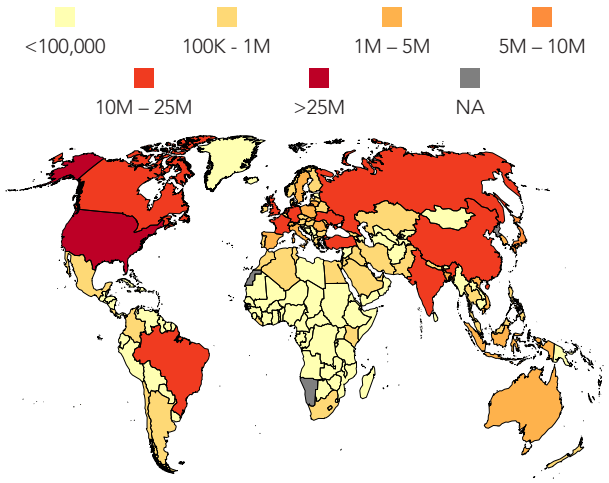
Le vecteur d'attaque dominant continue d'être l'injection SQL, qui représentait 50 % de toutes les attaques d'applications Web enregistrées au 4e trimestre, contre 47 % au 3e trimestre. Ces types d'attaques sont facilement automatisés et évolutifs, et ils resteront efficaces tant que les organisations n'auront pas pris les précautions appropriées, telles que la validation des saisies de l'utilisateur dans leur code.

Dans le domaine, les États-Unis continuent d'être le premier territoire, aussi bien source que cible, pour ce qui est des attaques d'applications Web, selon la plate-forme Akamai. Le pays a enregistré 238 millions d'attaques d'applications Web au 4e trimestre, contre 323 millions au 3e trimestre, ce qui représente encore plus de 10 fois plus que le deuxième au classement, le Brésil. Les États-Unis ont été la source de 132 millions d'attaques au quatrième trimestre, alors que les Pays-Bas sont en deuxième position avec 47 millions.

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

Le rapport *État des lieux d'Internet / Sécurité* du 4e trimestre 2017 réunit les données d'attaques de l'infrastructure mondiale d'Akamai et présente les recherches de nombreuses équipes de l'entreprise.

Pays à l'origine d'attaques d'applications Web, monde, 4e T 2017



[État des lieux d'Internet] / Sécurité

Équipe *État des lieux d'Internet / Sécurité*

Jose Arteaga, Akamai SIRT Lead, Data Wrangler — Analyse des attaques
Dave Lewis, Global Security Advocate — Activité des attaques DDoS et d'applications Web
Chad Seaman, Akamai SIRT — Analyse des attaques
Wilber Mejia, Akamai SIRT — Analyse des attaques
Alexandre Laplume, Akamai SIRT — Analyse des attaques
Larry Cashdollar, Akamai SIRT, Sr. Engineer — Web Vulnerabilities to Watch
Richard Willey, Sr. Data Scientist — How to Make Sense of a Planetary Scale Network
Elad Shuster, Security Data Analyst, Threat Research Unit
Jon Thompson, Custom Analytics

Équipe éditoriale

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

Contact

sotisecurity@akamai.com
Twitter : *@akamai_soti* / *@akamai*
www.akamai.com/stateoftheinternet-security

Télécharger le rapport complet

[État des lieux d'Internet] / Sécurité
Rapport complet au
4e trimestre 2017