[État des lieux d'Internet] / Sécurité

UNE ANNÉE PASSÉE AU CRIBLE

RÉSUMÉ : VOLUME 4, NUMÉRO 5

REMARQUES DE L'ÉDITEUR

Depuis novembre 2017, l'équipe de recherche d'Akamai a publié en moyenne plus d'un article par semaine. Ces articles portent sur des sujets aussi divers que les événements à venir, la communication de crise sur les menaces émergentes ou encore le rapport État des lieux d'Internet / Sécurité. Nous avons donc décidé de revenir sur notre travail et sur la manière dont il s'inscrit dans l'histoire de la sécurité de l'année écoulée. De plus, nous avons demandé à Andy Ellis, notre Chief Security Officer, d'émettre des hypothèses sur l'évolution des tendances pour 2019. Le texte suivant est un extrait de son article.

BUREAU DU RESPONSABLE DE LA SÉCURITÉ

> **Plus ça change, plus c'est la même chose —**
> Jean-Baptiste Alphonse Karr

Si une seule chose est vraie concernant les tendances de la sécurité Internet, c'est que les années se suivent et se ressemblent. En 1998, pendant l'opération Desert Fox, nos adversaires lancèrent une attaque de déni de service distribué (DDoS) afin d'exploiter une vulnérabilité *teardrop* et de mettre hors service des réseaux USCENTAF. À cette époque, j'étais l'ingénieur responsable de la défense de garde ce jour-là et je me souviens encore parfaitement de notre excitation lorsque nous avons identifié l'attaque, testé une configuration, puis repoussé l'attaque sur nos systèmes de sécurité de périmètre. Sur le plan stratégique, cela ressemble beaucoup à ce que nous faisons tous les jours dans nos centres d'opérations de sécurité. Seules l'échelle et l'automatisation changent.

À la veille de 2019, on peut raisonnablement penser que les schémas des dernières années vont globalement continuer d'évoluer dans la même direction.

Akamai
Experience the Edge

ATTAQUES DDoS EN FORCE

Les attaques DDoS constituent un bon point de départ, car les tendances de DDoS sont remarquablement stables. Ces attaques opèrent le long de deux axes différents : exploitation et bande passante. La *bande passante* est simplement la mesure du trafic qu'un adversaire peut générer à un moment donné. Historiquement, la taille des attaques majeures augmente d'environ 9 % par trimestre, soit un doublement tous les deux ans. Néanmoins, et c'est là le plus étonnant, cette croissance n'est pas continue. On enregistre un nouveau pic (dans les limites de cette courbe de 9 % par trimestre) chaque fois qu'un adversaire découvre une nouvelle façon de construire un botnet ou une réflexion, comme cela s'est produit lors de l'attaque Mirai ou des attaques par réflexion via memcached.

Entre deux pics, deux choses se produisent. Tout d'abord, les parties affectées (administrateurs système, opérateurs FAI) prennent des mesures visant à réduire le nombre de systèmes pouvant être potentiellement la cible d'une attaque. Deuxièmement, les adversaires se livrent une lutte acharnée pour le contrôle de ces ressources, ce qui entraîne une fragmentation progressive des botnets et une réduction de la taille des attaques individuelles.

Du point de vue de l'efficacité, cela n'est pas réellement préjudiciable à l'attaquant. En général, les styles de défense DDoS n'évoluent pas de manière linéaire. Les attaques majeures ont lieu à la périphérie du réseau, où résident des services d'Akamai comme Kona Site Defender ou Prolexic Routed. Les défenses de niveau intermédiaire sont installées au cœur des FAI, où elles assurent des services « clean-pipe » aux propriétaires de sites. Les défenses mineures que sont les solutions sur site existent quant à elles uniquement à l'intérieur des centres de données cibles. Pour un adversaire dont le botnet n'est pas assez puissant pour cibler une défense périphérique, une attaque contre une cible utilisant uniquement des défenses basées sur le centre de données peut s'avérer efficace, même à un centième de la taille initiale.

Compte tenu de la diversité des attaques DDoS basées sur la bande passante, il est intéressant de noter que la taille maximale des attaques semble être limitée par une courbe de croissance trimestrielle de 9 %. Intéressant, mais pas inexplicable. En effet, plutôt qu'une hypothétique limite naturelle, l'explication la plus probable est que la croissance sous-jacente de l'Internet restreint la capacité globale des botnets. La capacité d'Internet atténue la puissance potentielle d'une attaque DDoS. Plus une cible est éloignée des composants d'un réseau, moins il y aura de trafic à travers les liens encombrés entre la cible et la source de l'attaque.

Pour lire l'analyse détaillée d'Andy sur les attaques DDoS, les attaques de niveau d'application, les attaques par « credential stuffing », l'économie collaborative et les blockchains, téléchargez notre rapport **État des lieux d'Internet / Sécurité : Une année passée au crible**, Volume 4, Numéro 5.

À PROPOS D'AKAMAI

Akamai sécurise et fournit des expériences digitales pour les plus grandes entreprises du monde. L'Akamai Intelligent Edge Platform englobe tout, de l'entreprise au cloud, afin d'offrir rapidité, agilité et sécurité à ses clients et à leurs entreprises. Les plus grandes marques internationales comptent sur Akamai pour les aider à concrétiser leur avantage concurrentiel grâce à des solutions agiles qui développent la puissance de leurs architectures multi-cloud. Akamai propose des décisions, applications et expériences digitales au plus proche des utilisateurs, tout en maintenant les attaques et menaces environnantes éloignées. Les solutions de sécurité en périphérie, de performances Web et mobiles, d'accès professionnel et de diffusion vidéo du portefeuille d'Akamai s'appuient également sur un service client exceptionnel, des analyses et une surveillance 24 h/24, 7 j/7 et 365 j/an. Pour savoir pourquoi les plus grandes marques mondiales font confiance à Akamai, visitez www.akamai.com, blogs.akamai.com ou @Akamai sur Twitter. Vous trouverez nos coordonnées dans le monde entier à l'adresse https://www.akamai.com/fr/fr/locations.jsp. Vous pouvez également nous contacter au +33-185644654. Publication : 12/18.