Krebs en ligne après une attaque DDoS dopée par un réseau IoT (MAJ)

Le blog KrebsOnSecurity alimenté par le journaliste et chercheur en sécurité Brian Krebs est à nouveau accessible sur Internet après deux jours d'indisponibilités. Jeudi 22 septembre dernier, le site a été la cible d'une attaque par déni de service distribué (DDoS) d'une telle ampleur que la protection déployée par une filiale d'Akamai, Prolexic, n'a pas tenu la charge. Plus de 600 gigabits par seconde (Gbps) de trafic auraient submergé le site, soit deux fois le niveau atteint lors d'attaques précédentes déjà opérées contre le blog et d'autres sites, selon Akamai.

Comment expliquer un tel impact ? L'attaque massive qui a paralysé KrebsOnSecurity serait l'œuvre d'un botnet (ou réseau de machines zombies) essentiellement constitué d'objets connectés (IoT), selon Akamai. Le nombre de dispositifs connectés est encore *« inconnu »* à ce jour, mais il pourrait approcher le million, d'après Andy Ellis, le RSSI d'Akamai interrogé par *Network World*.

Or, avec 21 milliards d'objets connectés en circulation à horizon 2020, selon les prévisions du cabinet Gartner, la portée de botnets constitués d'objets peu ou mal sécurisés (tels que les bracelets connectés) pourrait être énorme. Et impose aux entreprises de mieux gérer le risque.

Google au secours de Krebs

L'attaque contre KrebsOnSecurity n'était pas une attaque par réflexion et/ou amplification, de sorte que toutes les requêtes HTTP ont été considérées comme légitimes. Akamai a déclaré que protéger le blog de Krebs contre ce type d'attaque est toujours possible, mais que le coût est beaucoup trop élevé pour un seul site (200 000 dollars par an ont été proposés par d'autres prestataires).

Le spécialiste du CDN et du Cloud a donc jeté l'éponge et retiré le site de ses serveurs. C'est Google qui fournit maintenant à Brian Krebs un service gratuit de protection contre les attaques DDoS : Project Shield. Un programme destiné à *« protéger les sites d'information et la liberté d'expression »*.

Notons, enfin, que l'hébergeur français OVH a également été la cible d'une série d'attaques DDoS la semaine dernière, rapporte son Pdg Octave Klaba. L'attaque se serait appuyée sur des caméras de surveillance mal protégées. Des dysfonctionnements momentanés du réseau ont été rapportés.

> *Last days, we got lot of huge DDoS. Here, the list of « bigger that 100Gbps » only. You can see the simultaneous DDoS are close to 1Tbps ! pic.twitter.com/XmlwAU9JZ6*
>
> *— Octave Klaba / Oles (@olesovhcom) September 22, 2016*

MAJ du 14/10/2016 à 10h30 : Akamai donne des précisions sur la protection apportée par ses services lors de l'attaque DDoS qui a ciblé KrebsOnSecurity le 22/09/2016. L'entreprise revient sur une phrase incluse dans l'article : *« la protection déployée par une filiale d'Akamai, Prolexic, n'a pas tenu la charge »*. Akamai déclare, à la suite de la publication de l'article en question, avoir *« bien vu et jugulé le trafic de l'attaque jusqu'à la fin du 3e jour [suivant son lancement] »*. À cette date, la société dit avoir cessé

d’assurer la sécurisation du site. L’entreprise a alors décidé de *« retirer ce client de sa plateforme »*, faute de pouvoir *« justifier les moyens et ressources utilisés »* auprès de ses clients payants. Akamai précise, enfin, avoir offert *« gracieusement ses services à ce client pendant 4 ans »*, puis, face à ses autres clients, ses employés et ses actionnaires, avoir pris *« la décision financière la plus juste possible »*.

Lire aussi :

Télégrammes : Microsoft anti-slack en novembre, Linkedin Learning est né, Brian Kerbs DDoSisé

DDoS à vendre : autopsie d’un service de hacking à la demande