Dyn submergé par un botnet de 100 000 objets connectés

Un responsable de Dyn a indiqué que l'attaque DDoS menée la semaine dernière et qui a bloqué plusieurs sites web (dont Reddit, Imgur, Twitter, GitHub , Soundcloud, Spotify, PayPal, etc.) avait pour responsable principal un botnet comprenant 100 000 objets connectés (principalement des caméras de surveillance) et infectés par le malware Mirai.

Le samedi 22 octobre, Dyn avait déjà confirmé qu'un botnet de type Mirai (infectant les objets connectés) avait participé à l'attaque. Elle n'avait par contre pas réussi à établir le nombre d'objets enrôlés. Dans un billet de blog, Scott Hilton, vice-président exécutif en charge des produits chez Dyn , explique : « *après une première analyse du trafic DDoS, la société a identifié 100 000 sources de trafic malveillant provenant de dispositifs compromis et contrôlés par Mirai* ».

Un simple débordement TCP et UDP

Scott Hilton en profite également pour apporter quelques détails techniques sur l'attaque. Les assaillants ont mené l'offensive via des paquets DNS TCP et UDP. Une attaque simplissime, mais qui a réussi à submerger les défenses de Dyn et causer ensuite des dommages sur l'IT interne. Avec cet afflux de requêtes DNS, Dyn a eu du mal à distinguer les demandes légitimes de celles malveillantes. Ce qui explique les « *dizaines de millions d'adresses IP* » source mises en avant par Dyn dans un premier message samedi, un total mis en doute par les experts en sécurité mais qui intégrerait donc à la fois les requêtes légitimes vers de grands sites du Web et le trafic issu du botnet.

« *Au cours d'un DDoS employant le protocole DNS, distinguer le trafic légitime de celui venant de l'attaque peut s'avérer compliqué* », confirme Scott Hilton. Et l'attaque peut générer des effets d'amplification dévastateurs. Chez Dyn, ces phénomènes ont abouti à « *un volume de trafic 10 à 20 fois supérieur à la normale au travers d'un grand nombre d'adresses IP* ». C'est la combinaison de l'attaque et de ce que le dirigeant qualifie de « *tempête de réémissions* » qui a poussé Dyn à donner une première estimation du nombre d'IP surestimé.

Une attaque menée par des amateurs

Dyn n'a pas indiqué la taille réelle de l'attaque en termes de volume de trafic, mais les spéculations vont bon train. Les experts estime que cet assaut doit dépasser l'attaque en déni de service dont OVH a été victime il y a quelques semaines. La société roubaisienne avait subi une attaque avec des pics à 1,1 Tbps. La plus grande attaque connue à ce jour et à laquelle l'hébergeur a bien résisté, grâce notamment à un système anti-DDoS maison basé notamment sur des puces reprogrammables (FPGA).

Si Dyn précise que l'enquête est toujours en cours pour en savoir plus sur l'attaque de la semaine dernière, certaines sociétés s'interrogent sur les personnes à l'origine de cette offensive. Flashpoint,

spécialiste dans la gestion du risque, écarte l'idée d'une opération commanditée par un Etat. Il penche plutôt pour des pirates amateurs (script kiddies) qui ont réussi à industrialiser le botnet Mirai. Un avis que partage Mikko Hyponen, expert en sécurité chez F-Secure. Il y a quelques semaines, le code source de ce botnet a été mis en ligne sur GitHub et a depuis intégré les boîtes à outils pour cyberattaquants.

A lire aussi :

DDoS : Le botnet IoT Mirai a bien participé au raid contre Dyn

IoT : les botnets Mirai ont doublé en quelques jours

crédit photo © F.Schmidt – shutterstock