DDoS : le code du botnet IoT Mirai mis en libre-service

La semaine dernière, Brian Krebs, journaliste spécialisé en sécurité, a vu son blog être la cible d'une attaque DDoS d'une rare violence. Avec des pointes à plus de 600 Gbit par seconde, le site n'a pas tenu et même Akamai a été obligé de le retirer de ses serveurs proxy. Au final, le blog Krebsonsecurity est de nouveau en ligne grâce aux efforts de Google et de son Project Shield.

Après une première analyse, cette attaque par saturation s'appuie sur un botnet d'objets connectés. Or il se trouve que cette attaque vient de faire surface sur les forums de cybercriminalité. Selon Brian Krebs, le code source du botnet composé de caméras et d'autres objets connectés a été mis en ligne. Ce botnet hérite du nom de Mirai et a œuvré aussi bien sur le blog de sécurité, mais aussi contre l'hébergeur Français OVH avec des pics de 1 Tbit par seconde. Il rejoint ainsi un autre botnet IoT nommé BashLight, moins fourni mais très efficace.

Code source publié = amélioration et diffusion

Une publication qui fait craindre le pire pour les spécialistes de la sécurité. En premier lieu, d'autres cybercriminels vont pouvoir travailler sur ce code et l'améliorer pour mener des attaques encore plus denses et plus ciblées. Ensuite, des botnets comme Mirai vont enrôler plus d'objets connectés et intégrer des kits d'exploits avec une ribambelle de variantes. Une inquiétude quand on sait que les cabinets d'analystes prédisent l'arrivée de plusieurs milliards d'objets connectés dans les 5 prochaines années.

Le point commun des botnets IoT réside dans l'utilisation de la faiblesse du protocole de connexion à distance, Telnet. Mais dans le cas de Mirai, il chiffre le trafic entre les objets connectés et le serveur de commandes et contrôle, le rendant plus difficile à détecter. Un effort doit donc être mené pour améliorer la sécurité de l'Internet des objets. Les constructeurs, éditeurs, et chercheurs avancent pour l'instant en ordre dispersé pour créer un standard en la matière. Pendant ce temps, les cybercriminels ont pris conscience du fort potentiel de l'IoT mêlé à des ransomwares.

A lire aussi :

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

IoT : les objets connectés, futur cauchemar pour les réseaux d'entreprise ?

crédit photo © Duc Dao – shutterstock