Le botnet IoT Mirai s'essouffle victime de son succès

Il est devenu l'épouvantail de la sécurité. En réussissant à enrayer le web américain pendant quelques heures, Mirai a gagné ses lettres de noblesse dans la communauté des cybercriminels. Et son succès a été confirmé par la mise en ligne de son code pour une plus grande diffusion. Mais contrairement à ce que l'on aurait pu penser, cette libération du code n'a pas eu comme effet d'amplifier la puissance des attaques, mais au contraire de « fragmenter » Mirai en réduisant le nombre d'objets connectés infectés.

Un constat établi par Flashpoint. La société de sécurité a montré ainsi qu'une attaque s'appuyant sur un botnet Mirai contre les sites des deux candidats à la présidentielle américaine s'est révélée un flop. Pour les experts de Flashpoint , « *le paysage de botnet IoT semble saturé avec trop de contrôleurs et pas assez de terminaux vulnérables* ». Il y a quelques semaines d'autres spécialistes estimaient que le botnet Mirai original comprenait plus de 300 000 objets connectés, principalement des caméras de surveillance et leurs enregistreurs numériques. Mais selon John Costello, cyber-analyste de Flashpoint sur la zone Asie-Pacifique, « *actuellement, le plus grand botnet Mirai actif est composé de 92 à 96 000 objets* ».

Une baisse de puissance, mais une infection encore vivace

Pour lui, la publication du code source de Mirai « *a provoqué une concurrence entre de nombreux pirates pour contrôler les objets connectés sensibles à Mirai* ». Dans le *modus operandi* de Mirai, le malware « *désactive les modes de communications qui ont servi à l'infection du dispositif, bloquant ainsi la porte à d'autres infections* ». En conséquence, il y a moins de terminaux à infecter et la concurrence des pirates fragmente le pouvoir du botnet Mirai. Et, donc, réduit sa capacité de nuisance.

Il faut ajouter aussi une meilleure capacité de réaction des opérateurs. Bob Rudis, chef de la sécurité chez Rapid 7 indiquait le 2 novembre dernier que Verizon et Comcast avaient constaté une baisse du trafic lié à Mirai, suggérant ainsi un début de remédiation. Le code source du malware comprend une seule voie pour définir le serveur C&C qui infecte le dispositif et donne les ordres d'attaques DDoS. Ce serveur peut être modifié rapidement en cas de danger, mais il est aussi plus visible par les opérateurs avec la possibilité de bloquer le trafic et éventuellement le débrancher. Mais si le serveur C&C disparaît, cela ne signifie pas que l'objet connecté est tiré d'affaire. Bien au contraire, s'il n'a pas été corrigé, il reste une cible pour un autre botnet Mirai.

A lire aussi :

Un botnet Mirai teste sa capacité de nuisance sur le Liberia

Des services de Level 3 interrompus : une nouvelle attaque DDoS Mirai ?

Photo credit: christiaan_008 via VisualHunt.com / CC BY-SA