Et si le botnet Mirai devenait éternel

Il ne faut jamais vendre la peau de l'ours avant de l'avoir tué. Cet adage peut s'appliquer parfaitement aux dispositifs IoT infectés par le botnet Mirai. Ce dernier a semé la terreur à la fin de l'année 2016 en enrôlant des terminaux (caméras de surveillance, enregistreurs vidéo, routeurs, etc.) pour mener ensuite de violentes attaques par déni de service.

Un contrôle à distance peut ressusciter Mirai

Jusqu'à présent, les malwares ciblant les périphériques IoT étaient supprimés quand l'utilisateur redémarrait l'équipement. Ce processus effaçait la mémoire de l'appareil et donc le logiciel malveillant. En théorie. En pratique, un scan des cibles potentielles a montré qu'après un court répit ces dernières étaient réinfectées.

Cette découverte a été réalisée par des chercheurs de la société Pen Test Partners qui ont scruté les failles de plus de 30 DVR (enregistreurs numériques). Une vulnérabilité a été trouvée permettant au malware de Mirai, ou d'autres logiciels malveillants ciblant les objets connectés, de survivre après un reboot des terminaux. « *Nous avons trouvé un moyen pour corriger à distance les terminaux vulnérables à Mirai* », explique Ken Munro, expert de Pen Test Partners dans un blog. Mais il ajoute que « *le problème de cette méthode peut être utilisée pour rendre Mirai persistant au-delà de la réinitialisation du système* ». Bien évidemment, Ken Munro et son équipe n'ont pas publié de détails sur cette faille pour éviter que des personnes mal intentionnées ne créent une version persistante de Mirai.

D'autres faiblesses pour une seconde vie de Mirai

En complément de leur trouvaille, l'équipe de Pen Test Partners a déniché d'autres vulnérabilités dans les DVR renforçant les pouvoirs de nuisance et d'existence de Mirai. Parmi ces faiblesses, il y a un port Telnet non standard (12323) que certains DVR utilisent à la place du port Telnet 23 standard. L'authentification est également source d'inquiétude. Des DVR disposent d'identifiants et de mots de passe pour le moins basiques : « admin/ [blanc] » et « admin/123456 ». Une marque de DVR non citée utilise des mots de passe modifiés quotidiennement, mais ils sont publiés en ligne sur sa documentation.

Ces différentes brèches accordent une seconde vie à Mirai. Ce dernier a commencé à perdre du terrain face à l'arrivée de concurrents, comme Persirai, BrickerBot ou Hajime. Par ailleurs, on peut espérer une embellie sécuritaire du côté des constructeurs de DVR. Récemment, Dahua Technologies a annoncé un partenariat avec Synopsys, spécialisée en cyber sécurité, pour améliorer les firmwares de ses équipements. L'année dernière, Hangzhou Xiongmai Technology avait décidé de rappeler plusieurs caméras IP vulnérables, mais pas les DVR vendus en propre et en marque blanche.

A lire aussi :

Hajime, Brickerbot : pas des malwares, mais des boucliers contre les botnets IoT Mirai ?

Le botnet IoT Mirai cible Windows pour mieux se répandre

Photo credit: Jason A. Samfield via VisualHunt / CC BY-NC-SA