Un nouveau botnet IoT prêt à faire éclater une cyber-tempête

Se dirige-t-on vers une catastrophe Internet majeure ? **Check Point** déclare avoir découvert un nouveau botnet massif au côté duquel **Mirai** ferait figure de hors-d'œuvre.

« *Un botnet massif est en train de préparer une cyber-tempête qui pourrait faire tomber l'Internet* », n'hésite pas à avancer l'éditeur de sécurité dans son alerte.

Baptisé « IoTroop », le malware a été détecté fin septembre et aurait déjà contaminé un grand nombre d'objets. Check Point évoque des millions d'objets, sans plus de précision pour l'heure.

Mais Les caméras IP sans fil de GoAhead, D-Link, TP-Link, AVTECH, Netgear, MikroTik, Linksys, Synology et d'autres sont les principales victimes. Tout comme le System Files Information Disclosure sous Linux.

Le calme avant la tempête

Si l'éditeur ignore l'origine de l'infection, elle semble néanmoins se propager directement depuis les objets eux-mêmes. Qui plus est, la propagation est mondiale, des Etats-Unis à l'Australie.

« *Jusqu' à présent, nous estimons que plus d'un million d'organisations ont déjà été touchées* », avance la société de sécurité IT qui a détecté IoTroop depuis sa solution anti-intrusion (IPS).

Et d'ajouter que « *nos recherches suggèrent que nous vivons maintenant le calme avant une tempête encore plus puissante [que Mirai]. Le prochain cyber-ouragan est sur le point de se produire.* »

Pour mémoire, Mirai avait généré une charge record de 623 Gbit/s enregistrée par Akamai. Une puissance phénoménale pour mener des attaques DDoS comme l'avait constaté OVH qui avait essuyé une charge de 1,1 Tbit/s.

Et 100 000 objets connectés enrôlés par Mirai avait également fait tomber les serveurs DNS du prestataire DYN privant une partie des Etats-Unis de sites comme Twitter, GitHub, Spotify ou Paypal pendant plusieurs heures.

Une campagne entièrement nouvelle

Si certaines caractéristiques analysées par Check Point laissent penser un lien possible avec Mirai, « *il s'agit d'une campagne entièrement nouvelle qui se répand rapidement dans le monde entier* », assure l'éditeur.

Les différentes tentatives lancées avec Mirai ont probablement permis aux personnes malveillantes d'affiner leur méthodologie.

Face à la menace, même si le dessein des cybercriminels reste inconnu, il convient de mettre en

place les défenses avant le début de l'attaque.

Sinon, des attaques en provenance de millions d'objets connectés risquent effectivement de se montrer dévastatrices pour les futures victimes.

Lire également
Et si le botnet Mirai devenait éternel
Malware : le botnet IoT Hajime grossit et inquiète
BrickerBot, le malware qui détruit les objets connectés

crédit photo : Image iAuthor:12019ID:bb4339c1982755-Pixabay