DDoS et IoT : Mirai s'en prend aux objets connectés de Sierra Wireless

Mirai est-il en train de gagner du terrain sur les réseaux d'objets connectés ? Quelques jours après que le journaliste Brian Krebs, spécialisé en sécurité, a révélé que le code source de Mirai est disponible en ligne, la société Sierra Wireless a lancé une alerte auprès de l'ISC-CERT, la division dédiée aux systèmes de contrôle industriels du centre d'alerte de sécurité américain.

Estampillée ICS-ALERT-16-286-01, l'alerte de l'entreprise canadienne spécialisée dans les solutions de connectivité cellulaire des objets précise simplement que les appareils dont les comptes de connexion par défaut n'ont pas été changés s'exposent au malware. D'autant que ces couples identifiants/mots de passe *« sont publiquement disponibles »*. Un appareil infecté par Mirai pourrait être intégré à un botnet pour lancer des attaques DDoS (Distributed Denial of Service) comme celles qu'ont subi le site Krebsonsecurity et des clients d'OVH, qui a dû essuyer des charges réseau allant jusqu'à 1,6 Tbit/s. Sont particulièrement visés les composants de connexion LS300, GX400, GX/ES440, GX/ES450 et RV50 de Sierra Wireless.

L'infection a commencé

L'alerte précise le mode opératoire de Mirai. Une fois en place sur la passerelle de communication, le malware s'installe en mémoire puis part à la recherche d'appareils vulnérables. Il fait ensuite remonter les informations récupérées via un serveur de commandes et contrôle (C&C). Conséquence : du trafic anormal sur les ports 23/TCP et 48101/TCP susceptibles d'alerter l'administrateur ou l'opérateur d'une recherche d'appareils vulnérables ou d'une attaque DDoS en cours. Pour y palier, Sierra recommande de rebooter l'appareil (pour détruire Mirai de la mémoire) et de changer de mot de passe.

L'ICS-CERT insiste sur le fait que la faille vient de la gestion de la configuration des appareils lors de leur déploiement. *« Il n'y a pas de vulnérabilité de logiciel ou matériel exploitée dans les appareils Sierra Wireless par le malware Mirai. »* Il n'en reste pas moins que l'infection est en cours. Dans une note publiée en parallèle le 4 octobre, le fournisseur confirme que *« le malware Mirai infecte des gateway AirLink qui utilisent le mot de passe par défaut d'ACEmanager (la console d'administration qui permet de gérer l'objet à distance, NDLR) et sont accessibles depuis l'Internet public. »*

30 000 passerelles Sierra concernées

L'entreprise canadienne ne précise pas le nombre de ses appareils potentiellement infectés. Selon le moteur de recherche spécialisé sur les objets connectés Shodan, plus de 30 000 passerelles AirLink sont accessibles depuis Internet. Essentiellement aux Etats-Unis. Combien avec le mot de passe d'administration par défaut ?

Mirai n'est pas le seul malware à exploiter les objets connectés pour opérer des attaques Internet. La semaine dernière, l'expert en sécurité qui avait mis la main sur Mirai a annoncé, sur son blog

Malware Must Die, avoir découvert Linux/NyaDrop, une nouvelle menace qui s'en prend aux architectures MIPS que l'on retrouve notamment au cœur des routeurs et autres éléments de réseau. Une grande carrière semble s'ouvrir pour les botnet IoT.

Lire également

DDoS : le code du botnet IoT Mirai mis en libre-service
Krebs en ligne après une attaque DDoS dopée par un réseau IoT
Une faille dans OpenSSH âgée de 12 ans fragilise l'IoT