Malware : le botnet IoT Hajime grossit et inquiète

Il y a une semaine le monde découvrait le botnet Hajime, qui signifie « commencer » (un mot bien connu des pratiquants de judo). Mais depuis, il a grossi et il effraie les experts en sécurité. Comme Mirai, il vise les objets connectés (routeurs domestiques, caméra de surveillance, enregistreur numérique) via des faiblesses de sécurité dans les protocoles et les firmwares. Il a été observé pour la première fois en octobre dernier à l'occasion d'attaques DDoS menées avec Mirai. A cette époque, les éditeurs de sécurité avaient concentré leur attention sur Mirai et avait délaissé Hajime.

Un botnet modulaire à des fins curatives

Symantec s'est penché sur ce botnet. Sur le *modus operandi*, une fois implanté sur les terminaux ciblés, via les ports Telnet ouverts ou l'exploitation de mots de passe par défaut, Hajime bloque l'accès à un certain nombre de ports (23, 7547, 5555 et 5358) afin de barrer la route à Mirai.

Un message du développeur de Hajime est là pour tranquilliser (ou tenter de tranquilliser) les personnes infectées : *« Je suis seulement un hacker blanc tentant de sécuriser quelques systèmes »*, écrit-il. Le but de Hijame serait donc de protéger les objets connectés.. en les infectant. Hijame utilise le protocole P2P pour communiquer avec les serveurs de commandes et contrôles.

Hajime s'étoffe et inquiète

Mais cet altruisme pourrait n'être qu'une façade et les spécialistes de la sécurité commencent à s'alarmer de sa potentielle force de frappe. En effet, les dernières estimations montrent que le ver a réussi à infecter 300 000 objets connectés et pourrait se transformer en un botnet IoT très puissant. Kaspersky et Radware ont également analysé Hajime et le considèrent comme très sophistiqué.

Mais l'aspect chevalier blanc est mis en doute. Pascal Geenens, Evangéliste Cyber Security pour Radware, explique à nos confrères de *Bleepingcomputer* qu si c'est « *juste un hacker blanc, alors pourquoi Hajime reste encore présent et continue à se développer ? Pourquoi il a nommé un process « atk » pour attaque et non découvrir ou scanner ?* ». Il ajoute : « *Il explore de manière très agressive les périphériques Telnet et WSDAPI vulnérables. Il ferme les ports exploités par Mirai, mais il les ouvre pour lui. Je ne suis pas sûr que l'on puisse parler de hacker blanc.* »

Dans le même registre, les experts s'inquiètent du risque que le botnet Hajime, contrôlé aujourd'hui par une personne avec de bonnes intentions ne soit à son tour piraté et que le réseau soit contrôlé par une personne ou un groupe moins philanthrope. Cette menace n'est pas à prendre à la légère, car Hajime est modulaire. Des pirates pourraient essayer de détourner les communications avec les serveurs de commandes et contrôles. Auquel cas, il faudra s'attendre à une recrudescence des attaques DDoS massives.

A lire aussi :

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

Le botnet IoT Mirai tente une incursion dans le bitcoin

crédit photo © F.Schmidt – shutterstock