Alerte sur Mirai, le malware créant des botnets d'objets connectés

Crédits : Hailshadow/iStock

Le malware Mirai s'en prend aux passerelles cellulaires, habituellement utilisées pour connecter certains équipements à Internet. Il est à l'origine de quelques-unes des plus vastes attaques distribuées par déni de service jamais enregistrées. Il fleurit malheureusement là où les consignes élémentaires de sécurité ne sont pas respectées.

Un signal d'alarme a été tiré jeudi dernier par l'ICS-CERT (Industrial Control Systems Cyber Emergency Response Team). Dans son bulletin, l'équipe indique que le constructeur Sierra Wireless est touché par un malware du nom de « Mirai ». Ses passerelles cellulaires AirLink sont attaquées et, une fois contaminées, sont capables de réunir une foule d'appareils connectés pour en faire une armée. En d'autres termes, un botnet d'objets connectés.

Ce sont plus précisément les modèles LS300, GX400, GX/ES440, GX/ES450 et RV50 qui sont concernés. Dans son propre bulletin de sécurité, Sierra Wireless indique que les infections réussissent quand l'interface de contrôle ACEmanager est utilisée sans que le mot de passe par défaut n'ait jamais été changé. Une règle de sécurité pourtant élémentaire en entreprise.

Des mots de passe par défaut non modifiés

L'entreprise indique : « *Sierra Wireless a confirmé les rapports selon lesquels le malware Mirai infecte les passerelles AirLink utilisant le mot de passe par défaut d'ACEmanager et accessibles depuis Internet* ». En utilisant la fonctionnalité de mise à jour du firmware, Mirai récupère une version vérolée qui simplifie ensuite les opérations de contrôle, donc d'attaque.

Les conseils sont donc simples pour les entreprises qui utilisent des produits Sierra Wireless, et plus globalement n'importe quel produit du même acabit. Le changement du mot de passe par défaut est la priorité. Le constructeur indique que les administrateurs doivent vérifier l'ensemble des accès extérieurs et couper tout ce qui n'est pas nécessaire, pour réduire la surface d'attaque. Si de tels accès sont requis, il conseille d'utiliser la redirection de ports, et surtout pas les fonctions DMZ Host et Public Mode.

La présence du malware se signale quant à elle de plusieurs manières, notamment un trafic anormal sur le port TCP 23. Le port TCP 48101 est utilisé par le malware pour tout ce qui touche aux instructions, émises et reçues. Si la passerelle est utilisée pour une attaque DDoS, le trafic sortant sera bien sûr très élevé. Pour information, OVH a indiqué que lors des plus fortes attaques de ces dernières semaines, des pics de 1 Tb/s avaient été enregistrés. Il rappelle également, tout comme Ars Technica récemment, que si Mirai a beaucoup été mis en avant, un autre malware – Bashlite – participait lui aussi aux manoeuvres.

D'autres rapports à prévoir

Cela fait environ un mois que Mirai sévit, avec une intensification probable à prévoir, due à la publication de son code sourceil y a deux semaines. Actuellement, les estimations font état d'au moins 1,2 million d'appareils contaminés, chacun pouvant contrôler un parc d'autres appareils, puisque ces passerelles sont notamment utilisées dans les chaines industrielles, les caméras de sécurité, etc.

En outre, il est probable que si Mirai réussit ce type de contrôle, d'autres malwares peuvent en faire autant, non seulement sur les produits Sierra Wireless, mais également sur d'autres équipements du même acabit. Il ne serait donc pas étonnant de voir arriver d'autres bulletins de sécurité dans les jours et semaines qui viennent

Publiée le 17/10/2016 à 14:00

Vincent Hermann Rédacteur/journaliste spécialisé dans le logiciel et en particulier les systèmes d'exploitation. Ne se déplace jamais sans son épée.