BrickerBot, un destructeur d'objets connectés qui agit… pour la bonne cause

Repérées en toute discrétion en mars dernier, les attaques de BrickerBot sont promises à une belle carrière. Le malware qui vise les objets connectés opérés par Linux « busybox », caméras IP et enregistreurs numériques en premier lieu, poursuit ses attaques massives. Attaques dont le seul objectif est, en apparence, de détruire les objets affectés en les rendant inopérants (l'intrus se charge de remplacer les programmes par des données aléatoires et coupe les connexions). Des attaques qualifiées de PDoS (Permanent Denial-of-Service, dénis de service permanent) ou encore «phlashing» (rinçage).

La carrière de BrickerBot est notamment suivie par Radware qui en mesure l'activité à l'aide de pièges à malwares (honeypot). Après les deux attaques du mois dernier, le fournisseur de solution réseau a constaté une nouvelle charge le 20 avril. En 12 heures, l'agent malveillant a réussi à créer une quinzaine de bots disséminés dans différentes régions du monde à partir de 1118 tentatives d'attaques constatées. Une quatrième attaque était également enregistrée en fin d'après-midi sur 90 cibles. Mais celle-ci a cessé un peu avant 21 heures.

2 millions d'objets attaqués

Selon Radware, les charges provenaient toutes de serveurs SSH Dropbear aux versions désuètes (SSH-2.0-dropbear_0.51, SSH-2.0-dropbear_2013.58, et SSH-2.0-dropbear_2014.63). Rappelons que, à l'instar de Mirai, BrickerBot s'attaque aux objets dont le port Telnet est ouvert et qu'il pénètre leur système en attaquant par force brute le système d'identification. Mais, contrairement à Mirai, le malware PDoS ne cherche pas à exploiter ces objets pour mener des attaques de plus grande ampleur (DDoS) contre des cibles précises.

Un schéma de fonctionnement inhabituel dont *Bleeping Computer* dévoile les rouages en interviewant l'auteur de BrickerBot, retrouvé sur un forum de hacker. Un hacker, agissant sous le pseudo de Janit0r sur le forum et se présentant comme éthique. Pas forcément évident quand on sait que le pirate revendique, chez nos confrères, plus de 2 millions d'objets connectés victimes de BrickerBot. Autant d'objets devenus inutiles donc.

Chimiothérapie pour objets connectés

Comment cet expert en informatique justifie-t-il son acte? *« Comme tant d'autres, j'ai été consterné par les attaques DDoS réalisées par des botnets IoT en 2016*, explique-t-il dans un email en partie reproduit par Bleeping. *J'avais la certitude que ces grandes attaques obligeraient les fabricants d'objets connectés à revoir leurs copies, mais quelques mois après ces attaques records, il est apparu que, malgré les efforts sincères de certains, le problème ne pouvait être résolu dans un délai acceptable par des moyens conventionnels. »*

Aux grandes menaces, les grands moyens semble donc dire Janit0r. Plutôt que des médecines

douces, le hacker a donc décidé de trancher dans le vif en n'hésitant pas à qualifier son projet de *« chimiothérapie »*. *« La chimiothérapie est un traitement lourd qu'aucun docteur sensé n'administrerait à un patient en bonne santé, mais Internet devenait gravement malade aux troisième et quatrième trimestres 2016 et la médecine douce s'est avérée inefficace »*, déclare-t-il.

BrickerBot va poursuivre sa carrière

Et le hacker ne semble pas vouloir mettre fin aux activités de BrickerBot. Du moins tant que des objets vulnérables resteront connectés à Internet. *« J'espère que les actions non conventionnelles de BrickerBot ont fait gagner une autre année aux gouvernements, aux vendeurs et à l'industrie en général afin qu'ils puissent maîtriser le cauchemar de la sécurité actuelle de l'IoT. »*

Janit0r revient également sur les capacités de son malware. Celui-ci s'avère plus complexe que les détails livrés par Radware. *« Chaque action du bot a un objectif statistiquement déterminé et ce qui est vu comme un comportement bugué ne l'est pas »*, assure le hacker. Il explique que BrickerBot, qui embarque 86 protocoles, s'attache avant tout à réparer les objets qui peuvent l'être. Leur destruction n'intervient que comme un plan B (comme BrickerBot), lorsque leur innocuité semble inatteignable.

Vu sous cet angle, BrickerBot agirait donc pour la bonne cause. Il n'en reste pas moins que les fabricants d'objets et leurs exploitants ont tout intérêt à mettre à jour la configuration de leurs appareils en suivant les recommandations de Radware et de l'ICS-CERT s'ils ne veulent pas prendre le risque d'avoir affaire à un malware IoT transformant leurs objets intelligents en un tas d'électronique inutilisable.

Lire également

BrickerBot, le malware qui détruit les objets connectés

Le botnet IoT Mirai cible Windows pour mieux se répandre

Face aux botnets IoT, les opérateurs vont devoir collaborer, selon Arbor

Photo credit: christiaan_008 via VisualHunt.com / CC BY-SA