BrickerBot, le malware qui détruit les objets connectés

Une nouvelle menace plane sur l'Internet des objets (IoT) : le PDoS (pour Permanent Denial-of-Service). *« Cette forme de cyber-attaque devient de plus en plus populaire en 2017, alors que des incidents impliquant des assauts matériellement dommageables se multiplient »*, annonce le fournisseur de solutions de cybersécurité Radware, sur son blog.

De quoi en s'agit-il ? Egalement appelé « phlashing » (rinçage), le PDoS s'attaque directement aux objets connectés là où les DDoS les détournent pour mener des attaques massives contre des cibles précises (réseaux, entreprises, Etats…). *« PDoS est une attaque qui endommage tellement un système qu'elle nécessite le remplacement ou la réinstallation du matériel »*, assure Radware qui a étudié la bestiole en détail.

1900 attaques en 4 jours

Sur 4 jours, le piège à malware (honeypot) de l'entreprise spécialisée dans l'équilibrage de charges a enregistré 1 895 attaques PDoS provenant de nombreux sites répartis dans plusieurs points de la planète (Europe, Amérique du Nord et du Sud, Asie, Afrique du Sud). Un réseau malveillant que Radware a baptisé BrickerBot. Moins d'une heure après le début de cette première attaque, une seconde (BrickerBot.2) surgissait, *« très similaire […] avec une intensité plus faible [333 attaques] mais plus poussée et à partir de sites d'émission dissimulés par des noeuds de sortie Tor »*, le réseau promettant la quasi-anonymisation de ceux qui l'empruntent.

L'objectif unique de BrickerBot consiste à compromettre les périphériques IoT et à corrompre leur capacité de stockage. Le mode opératoire du malware reste relativement basique. La compromission de l'objet se fait par force brute, via le protocole Telnet (comme pour le malware de DDoS Mirai), afin de pénétrer son système. Faute de chargement d'un binaire, les chercheurs de Radware n'ont pas réussi à définir les références utilisées pour casser les identifiants/mots de passe et n'ont pu constater qu'un usage régulier du couple 'root'/'root' et 'root'/'vizxv'. Mais la faible protection des identifiants de connexion sur les objets connectés ne devrait pas constituer une barrière très élevée à franchir pour BrickerBot.

Détruire le système de l'objet

Une fois entré dans le système de sa victime, le malware lance une série de commandes Linux qui visent à compromettre l'espace de stockage, puis à couper la connectivité Internet, affaiblir les performances de l'appareil et effacer ses fichiers, notamment les tables IP des firewall et les règles NAT. Autrement dit, à rendre l'objet complètement inopérant. Un mode opératoire que le développeur Timothy Britton confirme, avec quelques variantes néanmoins.

Ce mode opératoire vise donc particulièrement les objets dont le port Telnet est ouvert et publiquement exposé sur le réseau mondial, à l'image de ce qu'avait fait Mirai et d'autres botnets

IoT. Sont notamment ‘privilégiés’ les objets qui exposent le port 22 (SSH) exploités sous une version ancienne du serveur SSH Dropbrear. Selon Radware, qui s’est appuyé sur le moteur de recherche d’objets connectés Shodan, les appareils de réseau Ubiquiti sont particulièrement ciblés par BrickerBot. Y figurent des points d’accès et passerelles de réseau sans fil. De quoi potentiellement faire tomber un réseau.

Les deux attaques ont démarré le 20 mars à moins d’une heure d’intervalle. La première, BrickerBot.1 est aujourd’hui inopérante. La deuxième, BrickerBot.2, se poursuivait à l’heure où Radware publiait son billet, le 5 avril. Changer les identifiants de connexion et désactiver l’accès Telnet figurent parmi les premières recommandations que l’entreprise de sécurité avance pour permettre aux opérateurs d’objets connectés de sécuriser leur réseau.

Lire également

Le botnet IoT Mirai cible Windows pour mieux se répandre

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

Akamai dissèque l’attaque du botnet Mirai contre Krebsonsecurity

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