La méthode d'OVH pour démanteler les réseaux d'objets connectés zombies



Le premier hébergeur européen est une cible de choix pour les attaques par déni de service, de plus en plus menées via des objets connectés. OVH a donc créé un système pour déconnecter automatiquement les serveurs présents sur son réseau, avec les risques que cela comporte. Entretien avec Sébastien Mériot, l'un des ingénieurs derrière cet outil.

La lutte contre les *botnets*, ces larges réseaux d'appareils zombies, nécessite de traiter toujours plus de données, toujours plus rapidement. En décembre, la Botconf 2017 était placée sous le signe de l'automatisation et de l'intelligence artificielle (voir notre compte-rendu). Des chercheurs y présentaient autant des outils d'apprentissage que des systèmes capables de désassembler à la chaine des logiciels,

peu importe l'architecture sur laquelle ils reposent.

À cette occasion, Sébastien Mériot, ingénieur en sécurité chez OVH, a montré comment l'hébergeur automatise la suppression de serveurs de contrôle des botnets sur son réseau. « La première menace pour un fournisseur d'accès est une attaque DDoS [déni de service distribué, NDLR], pas un rançongiciel. Si le réseau tombe, notre activité meurt » déclarait-il alors. C'est ce danger que portent les malwares destinés à l'Internet des objets.

L'Internet des objets, cobaye idéal

« Nous avions choisi les malwares IoT, car c'est un domaine qui s'y prête très bien : la menace est en plein boom et les malwares sont généralement assez basiques » nous déclare Mériot, dans un entretien écrit. S'ils existent depuis une dizaine d'années, ils ont gagné leurs lettres de noblesse fin 2016, avec des campagnes fondées sur Mirai, dont celle contre Dyn, qui a rendu un nombre important de sites inaccessibles….[Lire la suite sur la source]

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été Les meilleurs conseils pour choisir vos mots de passe Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]