Pourquoi les objets connectés sont un danger pour l’Internet ?

Pourquoi les objets connectés sont un danger pour l’Internet ?

Plusieurs grands sites Internet ont vu leurs services perturbés vendredi soir suite à une attaque contre une partie de l'infrastructure du réseau global. Cette attaque est particulièrement inquiétante car elle n'est que la dernière manifestation d'un phénomène en plein essor : le piratage d'objets connectés mal sécurisés pour constituer des réseaux offensifs. Un fléau qu'il sera difficile d'endiguer.

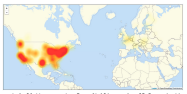
Une attaque de grande ampleur a eu lieu vendredi 21 octobre 2016, mettant hors service pendant quelques heures plusieurs grands sites Internet comme Amazon, Netflix, Twitter, Reddit, Spotify ou Tumblr. Ces sites n'étaient pas directement sous le coup d'une attaque, ils ont été les victimes collatérales d'une attaque contre Dyn, une entreprise dont les services font d'elle une infrastructure critique d'Internet : Dyn gère un service DNS (système de noms de domaine), qui permet de corréler un nom de domaine (comme « usine-digitale.fr ») en une adresse IP et vice versa.

UNE ATTAQUE BASIQUE MAIS SURPUISSANTE GRÂCE AUX OBJETS CONNECTÉS

Ce qui est notable ici, c'est qu'il ne s'agissait pas d'une attaque sophistiquée, soigneusement mise en oeuvre par un groupe d'experts. Non, il s'agissait d'une attaque par déni de service distribué (DDoS) – autrement dit une attaque ayant pour but de rendre un service indisponible en le noyant d'informations inutiles – s'appuyant principalement sur le botnet Mirai, qu'a identifié le cabinet d'analyse Flashpoint. Les botnets ne sont pas nouveaux, il s'agit de réseaux de machines dont un malware a pris le contrôle et qui peuvent être utilisés à tout moment pour mener une attaque coordonnée. Traditionnellement, les machines infectées étaient des ordinateurs dont les mises à jour de sécurité n'avaient pas été faites. Mais les progrès en matière d'antivirus et de solutions d'atténuation d'attaques DDoS limitent aujourd'hui sérieusement l'intérêt d'utiliser un botnet constitué d'ordinateurs (long et difficile à mettre en place) pour ce type d'opération (peu rentable car les rançons sont désormais rarement payées).

MIRAI, COMMENT ÇA MARCHE ?

La différence avec Mirai, c'est qu'il s'attaque aux objets connectés. Son *modus operandi* est on ne peut plus simple : il parcourt Internet en cherchant à se connecter à toutes les adresses telnet qu'il trouve avec une liste de 62 logins/mots de passe par défaut (dont le classique admin/admin). Une fois l'appareil infecté, Mirai en bloque certains ports pour empêcher qu'on en reprenne le contrôle. Le malware est basique, rapide, efficace, et surtout disponible gratuitement pour quiconque souhaite s'amuser avec, car son créateur en a rendu le code public. De plus, contrairement aux ordinateurs, un botnet d'objets connectés n'a aucune utilité réelle autre qu'effectuer des attaques par déni de service. Le fait que les objets connectés ont tendance à être allumés 24h/24 et 7j/7 facile aussi cet usage.



Impact de l'attaque contre Dyn, établie par Level3 Communications

CAMÉRAS ET ENREGISTREURS NUMÉRIQUES EN CAUSE

Le résultat est une arme dont la puissance est absolument démesurée par rapport à son accessibilité. En septembre 2016, le blog du journaliste spécialisé Brian Krebs avait été frappé par une attaque record atteignant un débit de 620 Gb/s. Une semaine plus tard, c'est l'hébergeur français OVH qui avait été visé, avec une puissance de frappe estimée à 1,5 Tb/s. L'attaque contre Dyn, survenue un mois plus tard, semble être à nouveau montée d'un cran. Quels sont les objets connectés utilisés par Mirai ? On y trouve beaucoup de caméras de surveillance et d'enregistreurs numériques (DVR), principalement fabriquées par une seule entreprise : Hangzhou XiongMai Technology. A noter que d'autres botnets pourraient également avoir participé à l'attaque. On connaît l'existence d'au moins un autre malware au fonctionnement similaire à Mirai, baptisé Bashlight.

PAS DE SOLUTION EN L'ÉTAT

Le problème est que ces appareils sont pratiquement impossible à protéger en l'état. Pour une partie d'entre eux, les identifiants sont codés « en dur » dans le firmware et ne sont pas modifiables. Et même pour les autres, le fait qu'ils utilisent le protocole telnet (en ligne de commande, sans interface graphique) les rend difficile à configurer pour les utilisateurs. D'après une analyse de Flashpoint, plus de 515 000 objets connectés seraient aujourd'hui vulnérables et susceptibles d'être incorporés dans un botnet. Certains experts ont proposé des solutions radicales, notamment de développer un malware plus rapide que Mirai, capable d'infecter un objet connecté vulnérable avant lui lors d'un redémarrage de ce dernier, et de le saboter pour le mettre définitivement hors service. Une mesure aussi drastique qu'illégale, mais qui souligne à quel point la situation désempare l'industrie.

Il y a eu beaucoup de mises en garde face au danger que représente l'Internet des Objets, mais, comme souvent, celles-ci n'ont servi à rien. Puisqu'il est clair que l'essor des objets connectés n'est pas prêt de s'arrêter, il est impératif que les acteurs majeurs de cette industrie mettent en place des normes et des bonnes pratiques au plus tôt, faute de quoi l'Internet des Objets continuera à scléroser l'Internet tout court, et ce de plus en plus souvent.

Original de l'article mis en page : Le retour des botnets ou pourquoi les objets connectés sont un danger pour l'Internet