La note du CESA
N°101
12 / 2016

Stagiaire Aurélien FRANÇOIS

Paralyser le Web via les objets connectés, quels enjeux pour la cyberdéfense ?

Le numérique a révolutionné une part importante de notre vie quotidienne. De plus en plus de supports que nous exploitons dépendent aujourd'hui de l'informatique et d'Internet. Cependant, les systèmes innovants, comme les objets connectés, manquent souvent de maturité en matière de sécurité. Une faille que savent exploiter les hackers pour pénétrer les systèmes que nous utilisons.

La cyberattaque massive contre le serveur *DNS* du 21 octobre 2016

Dans l'après-midi du 21 octobre 2016, les services *DNS* (*Domain Name System*) de la société américaine *Dyn* ont été l'objet d'une cyberattaque massive. Un service *DNS* permet à un utilisateur d'Internet de se rendre sur un site Web ; il fait le lien entre l'adresse IP de l'appareil et le nom de domaine du site. Les informaticiens de *Dyn* ont répertorié deux attaques, dites de « déni de service » (ou *DDoS* pour *Distributed Denial of Service*). L'objectif de ce type d'attaque est de saturer un serveur (qui héberge les sites web) en lui envoyant un flux colossal de requêtes, ce qui le rend temporairement inopérant. Des sites majeurs comme *Twitter*, *eBay*, *Netflix*, *CNN* ou encore le *New York Times* ont ainsi été temporairement inaccessibles.

Cette cyberattaque se distingue des autres *DDoS* pour deux raisons. La première réside dans la cible elle-même : en visant directement le *DNS* de *Dyn*, acteur majeur dans le domaine, l'attaque permet de paralyser non plus un seul serveur, mais des milliers de serveurs qui ont recours à ce *DNS* pour connecter les internautes. La seconde réside dans l'utilisation par le hacker d'objets connectés pour amplifier son attaque. Souvent faciles à pirater, les objets connectés (caméras de surveillance, téléphones, réfrigérateurs, etc.) génèrent une multitude de requêtes, qui sont alors redirigées vers le *DNS* visé.

Les limites de l'hyperconnectivité

Un mois plus tôt, l'hébergeur français de site Internet, OVH, a été l'objet d'une attaque similaire, d'une ampleur alors inégalée. Ces cyber-attaques montrent les limites de l'hyperconnectivité de notre société. Désormais, des bâtiments peuvent être entièrement connectés (du smartphone aux volets électriques, en passant par l'alarme du domicile). C'est un confort lié à la révolution domotique : un simple téléphone permet aujourd'hui de piloter un grand nombre d'objets domestiques.

Cependant, la diffusion exponentielle de ces systèmes expose leurs utilisateurs à une multitude de menaces. Les réseaux de connexion (wifi en particulier) sont facilement piratables. Une fois pénétré, le réseau est à la merci du groupe de hackers. Celui-ci peut lancer des attaques *DDoS* comme celles orchestrées à l'encontre de *Dyn* et d'OVH. Il peut également prendre le contrôle de n'importe quel objet connecté : ouvrir le gaz ou les robinets d'eau, lever les volets électriques, désactiver les alarmes, etc. De quoi provoquer nombre d'incidents domestiques ou faciliter une effraction, le tout à distance.

Les problématiques liées à la sécurisation des objets connectés

D'ici 2020, la société américaine *Cisco* estime qu'il n'y aura pas moins de 50 milliards d'objets connectés à Internet dans le monde ; or, le cabinet d'étude *Gartner* prévoit que d'ici la même année, plus du quart des cyberattaques identifiées seront liées à ces objets connectés au net. Une évolution qui annonce des enjeux majeurs en termes de sécurisation.

Considérés comme plus simples à pirater que les ordinateurs, les objets connectés constituent une faille de choix pour les hackers. Or, l'on constate aujourd'hui que de nombreux objets conçus et vendus sur le marché ne disposent pas ou peu de dispositifs de sécurité. Les concepteurs de réfrigérateurs ou encore de chauffages électriques ne semblent pas encore prêter une importance majeure à la sécurité de leurs produits. La raison est principalement financière : les coûts liés à la sécurisation de ces objets ne semblent pas justifiés dans certains secteurs. C'est pourtant là que doit débuter la cyberdéfense des objets connectés : tant que l'ensemble des industriels qui conçoit des objets connectés (ou pouvant le devenir) ne prend pas pleinement conscience des risques liés aux cyberattaques, les hackers parviendront à les pénétrer.

Les experts en informatique semblent unanimes : les cyberattaques de ce type vont évoluer et s'intensifier. Tout l'enjeu de la cyberdéfense des objets connectés résident donc dans leur sécurisation par les constructeurs, puis dans celle des réseaux qui les lient entre eux. L'impact médiatique de l'attaque du 21 octobre a peut-être accéléré la prise de conscience des industriels sur cette problématique.

Ces propos ne reflètent que l'opinion de l'auteur.