CYBERSÉCURITÉ
QUAND LA MACHINE A CAFÉ OUVRE LES PORTES DE LA MAISON

https://www.breizh-info.com/2019/07/19/123502/cybersecurite-quand-la-machine-a-cafe-ouvre-les-portes-de-la-maison
Article du 19/07/2019

Gartner prédit plus de 20 millions d'objets connectés dans le monde d'ici 2020, et autant de portes d'entrées pour les hackers. Les équipes d'Avast ont fait l'expérience du piratage d'une machine à café sous tous les angles, allant même jusqu'à transformer l'appareil en un outil de ransomware et en une passerelle vers un réseau domestique.

Martin Hron, chercheur en sécurité, chez Avast, explique comment s'est déroulé l'expérience et ce qu'elle révèle sur les opportunités que représentent les objets connectés pour les pirates informatiques :

« Imaginez votre pire cauchemar digital : vos objets connectés vous attaquent ! Pire que cela : votre fidèle et indispensable compagnon des premières heures de la journée, votre cafetière, se met en grève et refuse de vous servir un café ! Pour anticiper ce scénario, nous avons décidé d'explorer ses vulnérabilités. A l'instar de nombreux objets connectés, la machine à café qui a servi pour cette expérience a été livrée avec des paramètres par défaut et une connexion Wi-Fi, immédiatement prête à l'emploi. Aucun mot de passe n'étant requis pour se connecter, il a donc été très facile d'y injecter un code malveillant.

L'objectif n'était pas simplement de pirater une cafetière mais de sensibiliser et démontrer le potentiel d'attaque à l'encontre du monde de l'Internet des Objets (IoT), cible privilégiée des cybercriminels. De récentes recherches menées par Avast et l'Université de Stanford ont d'ailleurs montré que 40 % des foyers dans le monde possèdent au moins un appareil intelligent, et que 94 % des objets connectés sont fabriqués par moins de 100 fournisseurs différents, n'intégrant pas nécessairement la sécurité dès la conception ; ce qui entraîne l'existence de potentielles vulnérabilités similaires, susceptibles d'être exploitées dans le cadre d'attaques à grande échelle.

De nombreux terminaux IoT se connectent d'abord au réseau domestique via leur propre Wi-Fi, utilisé uniquement pour la configuration. Dans un monde idéal, les consommateurs protégeraient ce réseau par un mot de passe fort et complexe. Toutefois, de nombreux objets sont vendus sans mot de passe, et il est rare que les utilisateurs en définissent un. Il s'agit d'une vulnérabilité majeure, car le réseau Wi-Fi de l'appareil en question est public, et donc visible de tous, y compris des hackers qui peuvent y injecter un code malveillant.

Une fois introduits par cette porte d'entrée, ils sont en mesure d'atteindre d'autres objets de la maison puisque l'intégralité du réseau est accessible via un seul périphérique – et ainsi d'espionner les aspects les plus privés d'un individu et de collecter des données personnelles. Le scénario peut se révéler encore plus grave si un utilisateur ne s'aperçoit pas que des cybercriminels exploitent sa cafetière comme passerelle vers l'ensemble du réseau, et accèdent donc aux emails, aux données bancaires renseignées lors d'achats en ligne, au système de sécurité de la maison ou encore au babyphone. La plupart des consommateurs n'ont aujourd'hui pas conscience de la réalité de cette menace.

Des millions d'appareils IoT sans la moindre protection se trouvent actuellement sur le marché, soit autant de mauvaises habitudes de sécurité à changer ; à commencer par la modification du mot de passe par défaut du réseau Wi-Fi, mais aussi de tout nouveau périphérique. En outre, les objets connectés ne sont pas uniquement de simples gadgets : leur mise à jour régulière est indispensable au même titre que leur connexion seulement en cas d'utilisation.

Les vulnérabilités d'une simple cafetière connectée suffisent pour que des hackers accèdent à la vie privée de n'importe quel utilisateur. Il existe autant de risques que de solutions, c'est pourquoi il ne faut pas craindre l'explosion du nombre d'objets connectés, mais simplement prendre les mesures nécessaires pour protéger son réseau et ses données personnelles afin d'explorer en toute sécurité tout le potentiel de l'IoT, à l'abri des cybercriminels. »