Piratage d’ampoules connectées. Nouvelle porte d’entrée pour les hackers ?

Piratage d’ampoules connectées. Nouvelle porte d’entrée pour les hackers ?

Une équipe de chercheurs en sécurité informatique a réussi à prendre le contrôle d'ampoules connectées Philips Hue. Avant de s'en servir comme porte d'entrée pour accéder aux données des autres appareils reliés au même réseau.

Sésame, ouvre-toi ! Des chercheurs en sécurité informatique décrivent, dans une étude rendue publique ce jeudi 3 novembre, les attaques menées il y a quelques mois par leurs soins contre des ampoules connectées Philips Hue. Habituellement, ces objets connectés à un réseau Wi-Fi permettent à leurs utilisateurs de contrôler facilement et de personnaliser l'éclairage de leur domicile. Le résultat de l'expérience, relayée par le *New York Times,* est visible dans l'une des vidéos réalisées par l'équipe, qui avait préinstallé des ampoules sur un immeuble de Beer-Sheva, en Israël.

« À première vue, rien d'extraordinaire, mais imaginez des milliers ou même des centaines de milliers d'objets connectés à proximité les uns des autres », écrit le quotidien américain. Un programme malveillant créé par des hackers pourrait alors se répandre parmi ces objets en compromettant l'un d'entre eux, tel un agent pathogène. »

Et les conséquences sont quant à elle bien réelles. Ces hackers chevaliers blancs ont en effet été en mesure d'accéder aux données et même de contrôler tous les autres objets connectés à ce même réseau Wi-Fi.

Comment ? « Nous nous sommes contentés d'utiliser un équipement disponible à quelques centaines de dollars avant de parvenir à trouver cette faille, sans constater de mise à jour », détaillent les chercheurs. Alertée par ces derniers de la vulnérabilité de ses produits, la marque Philips leur a demandé de ne pas dévoiler publiquement les résultats de l'expérience avant que le problème soit résolu. Les utilisateurs des Philips Hue sont donc invités depuis le 4 octobre à télécharger une mise à jour pour renforcer leur sécurité. Mais, celle-ci est encore insuffisante, souligne l'un des experts, interrogé par Le Figaro.

« Les experts n'arrêtent pas d'alerter l'opinion publique »

Il y a un peu plus de deux semaines, de nombreux sites américains, comme Spotify, Amazon, eBay, Airbnb ou encore Netflixy, sont quant à eux restés inaccessibles pendant plusieurs heures, à la suite d'une attaque informatique. Pour mener à bien cet impressionnant piratage, les hackers avaient utilisé une armée de « machines zombies », constituée de centaines de milliers d'objets connectés, sans que leurs propriétaires ne s'en aperçoivent : des caméras de surveillance, des imprimantes, des lecteurs DVD, des babyphones, répartis un peu partout à travers le monde.

« Aujourd'hui, la plupart des appareils connectés au Web sont fabriqués en Asie, explique à LCI.fr Renaud Lifchitz, chercheur en sécurité informatique et expert en « Internet des objets » (IoT) chez Digital Security. Il existe de nombreux modèles et de nombreuses marques, mais la plupart utilisent le même logiciel ou un serveur identique. Il suffit pour le hacker de trouver une faille pour être capable de prendre le contrôle d'une large flotte d'appareils connectés ».

Depuis plusieurs années, les experts n'arrêtent pourtant pas d'alerter l'opinion publique sur le manque de sécurité de l'Internet des objets. « Aujourd'hui, la sécurité de la grande majorité des objets connectés est proche de zéro, abonde le blogueur Olivier Laurelli, alias Bluetouff, expert en sécurité informatique. Les fabricants ne se préoccupent pas de la sécurisation de leurs appareils connectés. Le plus important, pour eux, c'est de les lancer sur le marché avant les autres. »

[Lien vers l'Article de LCI]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Piratage : les ampoules connectées, une nouvelle porte d’entrée pour les hackers ? – LCI