

Kaspersky dévoile les limites de la maison connectée



Le spécialiste de la sécurité informatique Kaspersky vient de publier une étude mettant en lumière les failles de sécurité de plusieurs objets connectés pour la maison.

La société démontre comment le fameux Google Chromecast permet aux hackers de prendre contrôle de toute une maison 'connectée'.

Le rapport fait froid dans le dos...

Les rapports sur le manque de sécurité de certains objets connectés fleurissent sur internet, à l'instar de celui particulièrement alarmant publié par HP il y a quelques mois.

Malheureusement, ces problèmes de sécurité ne sont pas issus de la science-fiction, mais peuvent être à terme de vraies menaces pour les utilisateurs.

Kaspersky s'est intéressé aux objets connectés pour la maison, et en a choisi aléatoirement quatre différents qu'il a analysés :

la célèbre clé HDMI Google Chromecast, une caméra par IP connectée en Wi-Fi, une machine à café connectée ainsi qu'un hub de surveillance pour la maison. Il démontre ensuite pas-à-pas comment le Chromecast permet à un hacker de contrôler tous les autres appareils connectés dans la maison.

Forcer l'utilisateur à dévoiler le mot de passe du Wi-Fi Sans pour autant rentrer dans les détails techniques (disponibles dans le rapport), voici comment procède un hacker pour prendre contrôle de la maison :

- il utilise tout d'abord la vulnérabilité du Google Chromecast découverte en 2014 avec l'aide d'un Rickmote Controller. Cela lui permet ainsi de corrompre le contenu affiché sur la télévision et afficher un message d'erreur obligeant le propriétaire à changer le mot de passe du Wi-Fi, ou redémarrer le routeur.

- Une faille similaire a été découverte dans la machine à café connectée, qui n'a pas été nommée car la faille n'est toujours pas résolue.

- Une fois que le hacker possède le mot de passe du Wi-Fi de la maison, il peut ensuite facilement se connecter à la caméra de surveillance, et contrôler les allers et venues des personnes de la maison. Un cambrioleur peut ensuite s'introduire tranquillement dans la maison en utilisant un aimant suffisamment puissant et un vêtement capable de cacher la chaleur humaine. Pourquoi une telle tenue vestimentaire ? Les détecteurs de mouvements et de chaleur du hub de sécurité testé par Kaspersky pouvaient être facilement corrompus avec les méthodes assez simples d'utilisation.

Piratage : Une grand-mère se fait insulter par sa Smart TV ! Dans son communiqué, Kaspersky livre quelques conseils aux utilisateurs de tels produits pour se protéger un maximum, et éviter une attaque de grande ampleur.

A l'heure actuelle, réaliser un tel piratage reste cependant hautement complexe, et il est fortement probable que les cambrioleurs se contenteront encore pendant quelques temps de solutions plus classiques...

Ci-dessous, l'infographie qui résume la démarche de Kaspersky :



Lire la suite...

Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitements de données à caractère personnel (factures, contacts, emails...).

Même si remplir un formulaire de déclaration à la CNIL est gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.stuffi.fr/piratage-kaspersky-devoile-les-limites-de-la-maison-connectee/>