Quand les objets connectés contrôlent nos vies…

Quand les objets connectés contrôlent nos vies…

La sécurité est un enjeu majeur pour les objets connectés. Que ce soit dans le Quantified Self où les données relatives à la santé sont sensibles ou dans la domotique où les pirates peuvent prendre contrôle de la maison, les failles sont multiples.

Nous vous avions déjà parlé du hack du thermostat Nest lors de la Blackhat Conference, voici maintenant 5 autres cas avérés de piratage d'objets connectés. L'objectif n'est pas de vous faire peur, mais de simplement montrer que de nouveaux défis émergent pour toutes les sociétés qui s'y lancent.

Le compteur électrique qui coupe le courant
Une étude réalisée par deux experts en sécurité a montré de sérieuses lacunes dans les derniers compteurs d'électricités intelligents mis sur le marché pour répondre aux nouvelles normes du gouvernement espagnol. Les deux spécialistes ont ainsi démontré qu'il était possible de couper le courant chez les propriétaires (potentiellement pour créer un gros black out) ou trafiquer les compteurs pour fausser les factures. Grâce à un système d'infection en cascades, il serait même possible de remonter jusqu'aux centrales électriques. Sans donner le nom du fournisseur de compteurs chez qui la faille a été découverte, on sait cependant qu'il s'agirait d'un des gros acteurs du marché en Espagne que sont Endesa, Iberdrola ou E.ON.
L'Union Européenne a lancé un programme pour inciter les habitants à développer l'usage du compteur d'électricité intelligent, dans l'objectif d'économiser 3% d'énergie supplémentaires d'ici à 2020. A cette date, ce sont deux tiers des européens qui devraient en avoir installé un (sous condition qu'ils ne représentent pas de faille aussi importante…).

L'ampoule connectée qui découvre les mots de passe Wi-Fi
La société Context a exposé une faille de sécurité dans une ampoule connectée : la Lifx Wi-Fi. En parvenant à accéder à l'ampoule, elle a réussi à récupérer et décrypter les informations de configuration du réseau. L'équipe qui avait déjà trouvé des failles dans des imprimantes ou des moniteurs pour bébés a accédé au firmware de l'ampoule en étudiant le microcontrôleur afin de comprendre le mécanisme de cryptage de l'ampoule.
Le responsable recherche chez Context a déclaré « Pirater l'ampoule n'est pas simple, mais ne nécessite pas non plus d'avoir des connaissances trop complexes en matière de hack ». Il précise que ces vulnérabilités peuvent facilement être comblées en travaillant avec les développeurs Lifx. Il a déjà vu des cas plus complexes…

Le moniteur vidéo qui insulte bébé
Un couple américain habitant de l'Ohio a entendu une voix inconnue dans la chambre de leur bébé en août 2013. Il s'agissait d'un hacker qui avait réussi à prendre le contrôle de la caméra pour surveiller le bébé. Selon ABC News, la voix proférait des insultes au bébé.
Le père du bébé avait pourtant pris des précautions, notamment en donnant des mots de passe à son routeur et la caméra et en utilisant un pare-feu. La caméra était une Foscam. La société a rapidement sorti une mise à jour permettant d'éviter de nouveaux désagréments. Malheureusement, tous les utilisateurs n'ont pas mis à jour leur caméra de surveillance de bébé, à l'instar de la famille Schreck chez qui l'incident s'est reproduit en avril 2014. Les réactions en vidéo :

La box TV qui menace les grands-mères
A croire que cela ne se passe qu'aux Etats-Unis, voici l'histoire d'une grand-mère de la ville d'Indianapolis qui a eu la mauvaise surprise de voir des messages vulgaires apparaître sur sa télévision après que sa box TV AT&T ait été piratée. Alana Meeks a rapidement changé de box en n'espérant plus jamais revoir ces messages menaçants, rien n'y a fait. La police est intervenue et a pris notes des injures proférées à son encontre sur la télévision.
AT&T a immédiatement déclaré rechercher les causes de ce piratage, mais aucune nouvelle information n'a été officialisée depuis. On ne sait finalement pas si Mme Meeks a rallumé une télévision depuis.

Le frigo connecté spammeur
Le premier cas de frigo qui envoi du spam a été découvert en Californie au début de l'année. Il faisait partie d'un parc de plus de 100 000 appareils dont les pirates se servaient pour leur spam, avec des ordinateurs, des smart TV et des médias center. Plus de 750 000 emails ont été envoyés depuis ces appareils, dont 75% par les ordinateurs et le reste par des objets pour la maison reliés à internet.
Bref, autant d'exemple pour montrer que les objets connectés sont aujourd'hui vulnérables à ce genre d'attaques. Evidemment, avec le nombre de ces appareils qui va en s'accroissant, il faudra que les fournisseurs de technologie redoublent de vigilance pour assurer la sécurité de leurs clients. On se rappelle que HP a publié il y a quelques mois une étude qui montrait des résultats effarant sur les objets connectés : ce ne seraient pas moins de 250 vulnérabilités qui auraient été découvertes dans les 10 objets connectés les plus populaires du moment.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.stuffi.fr/objets-connectes-exemples-piratages-insolites/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+Stuffi+(Stuffi+-+L%27actualit%C3%A9+des+objets+connect%C3%A9s