OVATION AMERICAS

Avril 2022 Infolettre

Vos appareils vous espionnent-ils? (Partie 1)

De plus en plus d'objets et d'appareils dans la maison sont maintenant connectés à Internet, ce qui les rend potentiellement à risque d'être piratés.

Des téléviseurs connectés à Internet, des jouets, des réfrigérateurs, des fours, des caméras de sécurité, des serrures de porte, des trackers de fitness et des lumières, le soi-disant « Internet des objets » (IoT) promet de révolutionner nos maisons.

Mais cela menace également d'accroître notre vulnérabilité aux actes malveillants. Les failles de sécurité dans les appareils IoT sont courantes. Les pirates peuvent exploiter ces vulnérabilités pour prendre le contrôle des appareils, voler ou modifier des données et nous espionner.

En reconnaissance de ces risques, de nombreux gouvernements ont introduit un nouveau code de pratique pour encourager les fabricants à rendre les appareils IoT plus sûrs. Le code fournit des conseils sur les mots de passe sécurisés, la nécessité de correctifs de sécurité, la protection et la suppression des données personnelles des consommateurs et le signalement des vulnérabilités, entre autres choses.

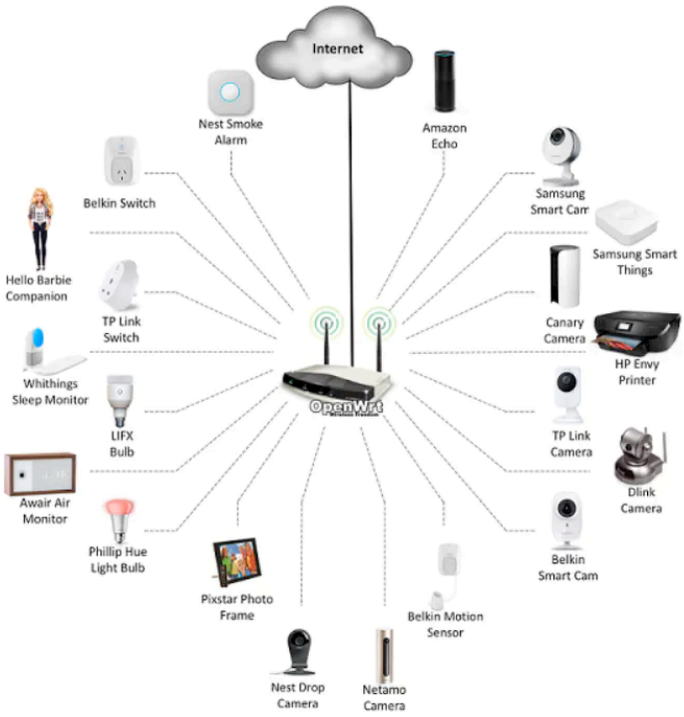
Le problème est que la plupart du temps, le code est volontaire. D'autres expériences, comme au Royaume-Uni, suggèrent qu'un code volontaire sera insuffisant pour offrir les protections dont les consommateurs ont besoin. En effet, cela pourrait même augmenter les risques, en berçant les consommateurs dans un faux sentiment de sécurité quant à la sécurité des appareils qu'ils achètent.

De nombreux appareils IoT ne sont pas sécurisés

Les appareils IoT conçus pour les consommateurs sont généralement moins sécurisés que les ordinateurs conventionnels.

En 2017, l'Australian Communications Consumer Action Network a chargé des chercheurs de l'Université de Nouvelle-Galles du Sud de tester la sécurité de 20 appareils électroménagers capables d'être connectés et contrôlés via Wi-Fi.

Ceux-ci comprenaient une télévision intelligente, un haut-parleur portable, un assistant vocal, une imprimante, un moniteur de sommeil, un cadre photo numérique, des balances de salle de bain, une ampoule, un interrupteur d'alimentation, un détecteur de fumée et une poupée parlante Hello Barbie.



Bien que certains appareils (y compris la Barbie) se soient avérés relativement sûrs en termes de confidentialité, tous présentaient une forme de faille de sécurité. Beaucoup « ont permis des atteintes potentiellement graves à la sûreté et à la sécurité ».

Ce que cela pourrait potentiellement signifier, c'est que quelqu'un pourrait, par exemple, pirater le réseau Wi-Fi d'un ménage et collecter des données à partir d'appareils IoT. Cela peut être aussi simple que de savoir quand les lumières sont allumées pour déterminer quand une maison peut être cambriolée.

Quelqu'un avec une intention plus malveillante pourrait allumer votre four tout en éteignant les détecteurs de fumée et autres capteurs.

Risques pour les consommateurs et la société

Les facteurs conduisant à une mauvaise sécurité dans les appareils Iot incluent le désir des fabricants de minimiser les composants et de réduire les coûts. De nombreux fabricants de biens de consommation ont également peu d'expérience des questions de cybersécurité.

Combiné au fait que de nombreux consommateurs ne sont pas assez avertis sur le plan technologique pour apprécier les risques et se protéger, cela crée la perspective d'exploiter les appareils IoT.

Sur le plan personnel, vous pourriez être espionné et harcelé. Des photos ou des informations personnelles pourraient être exposées au monde ou utilisées pour vous extorquer.

Au niveau sociétal, les appareils IoT peuvent être détournés et utilisés collectivement pour fermer des services et des réseaux. Même compromettre un appareil peut permettre de pirater l'infrastructure connectée. Il s'agit d'une préoccupation croissante à mesure que de plus en plus de personnes se connectent aux réseaux de travail à partir de leur domicile.

Ces nouveaux appareils IoT nous facilitent souvent la vie. Les appareils IoT peuvent améliorer l'efficacité, la commodité, la productivité ou la qualité globale de nos vies.

Mais, il y a toujours un compromis entre leur valeur d'amélioration de la vie et une perte potentielle de la vie privée. Bon nombre des appareils IoT pratiques que nous utilisons à la

maison, au travail, dans la voiture ou partout où nous allons **posent également des risques d'espionnage**. C'est le cas de trois appareils IoT récemment introduits..

Apple Air Tags

Un appareil IoT qui fournit un moyen facile de suivre vos objets. (p. ex. portefeuille, clés, vélo, etc.)

Fonctionnalités:

- Se connecte à votre appareil Apple pour vous aider à localiser les éléments que vous avez marqués avec l'Apple AirTag
- Agit comme une balise en émettant un son afin que vous puissiez localiser vos objets étiquetés
- Envoie un signal Bluetooth détecté par les appareils à proximité dans le réseau Localiser et envoie l'emplacement de l'AirTag à iCloud
- Il utilise le réseau Find My (avec plus de 100 millions d'appareils iPhone, iPad et Mac dans le monde entier) pour vous aider à localiser vos objets étiquetés
- Utilisez Precision Finding avec un Apple iPhone 11 ou version ultérieure en conjonction avec l'app Localiser et Siri pour trouver vos objets marqués.

Risques:

1. Un espion peut connecter un AirTag à son appareil Apple, puis déposer l'AirTag dans votre poche, sac à main, sac à dos, voiture, etc. Ils peuvent suivre vos allées et venues à portée de l'étiquette dans une fenêtre de 8 à 24 heures à l'aide de

leur iPhone. L'espion peut capturer votre emplacement, vos mouvements, votre adresse de résidence et vos lieux fréquemment visités.

2. L'AirTag peut être ouvert et reprogrammé à des fins malveillantes. Oui, les chercheurs en sécurité ont piraté l'AirTag en moins de 10 jours.
3. Si vous utilisez un appareil Android, la seule façon de connaître la présence d'un AirTag à proximité est le son émis par l'Apple AirTag. Le son commence après une période d'inactivité (plage de 8 à 24 heures). Mais, si vous ne pouvez pas entendre le son émis par l'AirTag et que vous n'utilisez pas d'iPhone, l'espion peut continuer à vous suivre pendant environ un an, ce qui concerne la durée de vie de la batterie. Une application Tracker Detect pour Android maintenant disponible chez Apple!

Amazon Sidewalk

Un appareil IoT qui crée un réseau « maillé » partagé d'appareils interconnectés.

Fonctionnalités:

- Crée un réseau à faible bande passante à l'aide de périphériques Sidewalk Bridge
- Partage une partie de votre bande passante Internet avec un pool qui fournit les services à vous/vos voisins (bande passante maximale 80Kbps, 500 Mo par mois par limite client).
- Fourni par Amazon sans frais pour les clients

- Simplifie la configuration des nouveaux appareils
- Étend la plage de travail à faible bande passante des appareils tels que les trackers (par exemple, Tile)
- Peut aider les appareils à rester en ligne même lorsqu'ils sont hors de portée de votre Wi-Fi domestique

Risques:

1. Un espion / pirate se connecte au réseau Amazon Sidewalk, utilise des logiciels malveillants pour pénétrer les appareils et mène des activités illégales avec votre appareil.
2. Le réseau d'un voisin n'est pas correctement sécurisé, mais il est connecté à Amazon Sidewalk. Un pirate informatique place un ransomware sur le réseau / les appareils du voisin et le ransomeware se propage à d'autres appareils connectés au trottoir Amazon.
3. Un pirate pénètre dans un réseau connecté à Amazon Sidewalk et l'utilise pour accéder aux informations sur les appareils connectés.

Audio Wow+

Appareil IoT qui est un mini microphone sans fil avec des effets sonores.

Fonctionnalités:

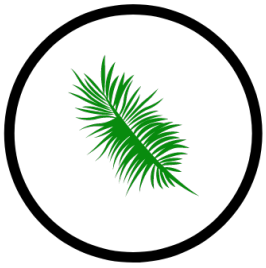
- Téléphone portable connecté directement
- Microphone intégré
- Surveillance en temps réel
- 4 niveaux de réduction du bruit

- Annuler et remplacer les voix d'origine
- Enregistre les appels téléphoniques et transcrit le contenu de l'appelant et du récepteur séparément pour faciliter l'édition

Risques:

1. Peut être utilisé pour des enregistrements subreptices car sa petite taille le rend facile à dissimuler.
2. Enregistrez les deux extrémités de la conversation. La plupart des appareils n'enregistrent que la moitié de la conversation où le microphone est présent.
3. Il est possible que les enregistrements vocaux soient modifiés pour créer des enregistrements ou des preuves de conversations qui n'ont pas eu lieu.

Que peut-on faire pour arrêter la cyber-écoute / les menaces IoT?



Il est essentiel de protéger vos informations précieuses contre les menaces IoT. Alors, comment pouvez-vous empêcher que votre sécurité ne soit compromise?

Avoir des balayages TSCM / CYBER TSCM PÉRIODIQUES conçus pour détecter les appareils mobiles malveillants, les téléphones portables cachés et autres dispositifs d'écoute et de piratage sans fil et confirmer que personne n'a compromis vos propres appareils personnels.

Si vous voulez vous assurer que votre vie privée est sécurisée, n'hésitez pas à nous contacter dès aujourd'hui! A: info@ovationamericas.com ou via notre site web au:

www.ovationamericas.com

La sécurité et la confidentialité sont une question de bonnes habitudes personnelles. Continuons à apprendre et à rester à jour sur les questions de cybersécurité pour nous donner les meilleures chances d'éviter les piratages et les escroqueries coûteuses.

OVATION
AMERICAS