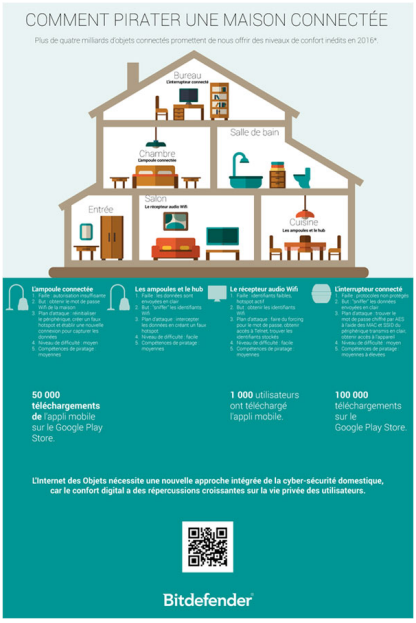
Est-ce facile de pirater une maison connectée ?

	Est-ce facile de pirater une maison connectée ?

L'analyse révèle que les mécanismes d'authentification de ces objets connectés peuvent être contournés et donc exposer potentiellement les foyers et leurs occupants à une violation de leur vie privée. L'Internet des Objets pose des problèmes de sécurité spécifiques, et par conséquent, nécessite une nouvelle approche intégrée de la cyber-sécurité domestique, qui passe de la sécurité centrée sur le périphérique à une solution capable de protéger un nombre illimité d'appareils et d'intercepter les attaques là où elles se produisent : sur le réseau.



Les chercheurs des Bitdefender Labs ont réalisé une étude sur quatre périphériques de l'Internet des Objets (IdO) destinés au grand public, afin d'en savoir plus sur la sécurisation des données de l'utilisateur et les risques dans un foyer connecté :

1. **L'interrupteur connecté WeMo Switch** qui utilise le réseau WiFi existant pour contrôler les appareils électroniques (télévisions, lampes, chauffages, ventilateurs, etc.), quel que soit l'endroit où vous vous trouvez ;
2. **L'ampoule LED Lifx Bulb** connectée via WiFi, compatible avec Nest ;
3. Le kit **LinkHub**, incluant des**ampoules GE Link et un hub** pour gérer à distance les lampes, individuellement ou par groupes, les synchroniser avec d'autres périphériques connectés et automatiser l'éclairage selon l'emploi du temps ;
4. **Le récepteur audio Wifi Cobblestone de Muzo** pour diffuser de la musique depuis son smartphone ou sa tablette, via le réseau WiFi.

L'analyse révèle que les mécanismes d'authentification de ces objets connectés peuvent être contournés et donc exposer potentiellement les foyers et leurs occupants à **une violation de leur vie privée**. Les chercheurs de Bitdefender sont parvenus à découvrir le mot de passe pour accéder à l'objet connecté et à intercepter les identifiant et mot de passe WiFi de l'utilisateur.

Les **failles identifiées** par l'équipe de recherche Bitdefender concernent des protocoles non protégés et donc vulnérables, des autorisations et authentifications insuffisantes, un manque de chiffrement lors de la configuration via le hotspot (données envoyées en clair) ou encore des identifiants faibles.

L'IdO pose des problèmes de sécurité spécifiques, et par conséquent, nécessite **une nouvelle approche intégrée de la cyber-sécurité domestique**, qui passe de la sécurité centrée sur le périphérique à une solution capable de protéger un nombre illimité d'appareils et d'intercepter les attaques là où elles se produisent : **sur le réseau**.

Si des marques comme Philips et Apple ont créé un écosystème verrouillé, **l'interopérabilité reste essentielle** à ce stade du développement des nouveaux objets connectés. Il est donc plus que temps que les constructeurs prennent en compte nativement la sécurité dans le développement de leurs différents appareils… [Lire la suite]

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

Source : *Comment pirater une maison connectée ?*