SmartThings de Samsung, une porte ouverte sur les failles

Dans quelle mesure la maison connectée représente-t-elle un risque en matière de sécurité ? Earlence Fernandes et Atul Prakash, chercheurs à l'université du Michigan, se sont intéressés à la question.

En association avec Jaeyong Jung, de Microsoft, ils ont choisi de mener des tests sur la plate-forme SmartThings de Samsung, qui prend en charge plus d'une centaine d'équipements, avec un kiosque d'un demi-millier d'applications.

Dans l'absolu, les expérimentations sont édifiantes : les trois chercheurs sont parvenus à déclencher, à distance, l'alarme associée à un détecteur de fumée. Mais aussi à désactiver le système d'allumage et d'extinction automatique de l'éclairage destiné à dissuader les voleurs en cas d'absence. Et à implanter une porte dérobée dans une serrure électronique tout en récupérant le code PIN.

L'analyse n'a pas été facile, SmartThings s'appuyant sur un environnement cloud fermé et sur des protocoles propriétaires pour assurer la communication entre les objets connectés, les passerelles (ZigBee, Z-Wave, Wi-Fi…) et l'application pour téléphones mobiles.

Une multitude de failles

Une analyse statique combinée à des examens manuels de code source a permis de détecter plusieurs failles qui feront l'objet d'une présentation détaillée dans le cadre du symposium sur la sécurité et la vie privée que l'IEEE organise du 23 au 25 mai prochaines à San José (Californie).

Premier problème : les privilèges accordés aux applications. Sur 499 de ces « SmartApps », 55 % requièrent plus de permissions qu'elles n'en auraient réellement besoin. Et 42 % ont des droits qui ne sont pas explicitement spécifiés à l'utilisateur.

Autre souci : dès qu'une application bénéficie de l'accès à au moins une fonction d'un appareil connecté, elle peut, sans davantage de privilèges, accéder à tous les messages émis par cet appareil. Une application sans aucune permission peut aussi y accéder, simplement via un identifiant d'appareil facilement récupérable.

Sésame ouvre-toi

Dans la pratique, les chercheurs ont notamment exploité, sur le serveur SmartThings, une faille de type « open redirect » qui leur a permis de mettre une backdoor dans une serrure électronique. La faute à une application – non citée – dans laquelle on peut trouver un code secret normalement inaccessible.

L'attaque implique l'envoi d'un lien à la victime, typiquement par un e-mail d'apparence légitime au

nom du service client SmartThings. Une page s'ouvre et l'utilisateur renseigne ses identifiants… qui sont communiqués aux pirates. Lesquels peuvent alors se connecter à l'administration cloud et ajouter un code PIN.

Dans leur rapport (document PDF, 19 pages), Fernandes, Jung et Prakash évoquent d'autres scénarios d'attaque plus compliqués à mettre en place. La victime doit, en l'occurrence, télécharger, via le *store* SmartThings, un *malware* présenté comme une application légitime destinée à suivre le niveau de batterie des équipements connectés.

Pour sa défense, Samsung met cette complexité en avant : l'attaque suppose qu'une app malveillante ait pu se glisser sur le *store* SmartThings ; or, un processus de soumission existe, avec une vérification du code, souligne *ITespresso.fr*.

Du côté des chercheurs, on émet des doutes sur la capacité des équipes de SmartThings à repérer leur app malicieuse, les commandes étant logées côté serveur…

A lire aussi :

IoT : le SDK Artik 10 de Samsung bientôt en vente
Intel renforce la sécurité de l'IoT avec Yogitech

Crédit photo : exopixel – Shutterstock.com