Deux chercheurs ont verrouillé un thermostat connecté avec un ransomware

Deux chercheurs en sécurité ont montré samedi durant la Def Con qu'il était possible d'introduire un ransomware dans un thermostat connecté, aboutissant au verrouillage de ce dernier. Il ne s'agit donc pas d'une menace réelle, mais d'une preuve que certaines craintes autour des objets connectés sont fondées.

Depuis plusieurs années, de nombreux experts en sécurité mettent en garde contre les dangers inhérents aux objets connectés. De nombreuses fonctionnalités reliées à Internet ont été mises en place pour simplifier la vie des utilisateurs autant que l'interconnexion avec d'autres produits et services. Mais dans bon nombre de cas, ces capacités ne sont pas assez sécurisées : des accès administrateurs sont laissés en place, des mots de passe faibles par défaut sont utilisés, et ainsi de suite.

Un bitcoin pour retrouver la bonne température

Sans forcément parler d'une future « apocalypse » des objets connectés, il est à craindre des séries d'attaques qui se prolongeront pendant plusieurs années, le temps que le marché prenne la mesure des risques encourus. C'est ce que deux chercheurs, Andrew Tierney et Ken Munro, ont souhaité démontrer samedi durant la Def Con. Ils ont pour cela piraté un thermostat connecté.

Travaillant tous deux pour la société de sécurité Pen Test Partners, ils ont montré comment ils s'étaient introduit dans le produit pour y injecter un ransomware. Il ne s'agissait bien entendu pas d'un « vrai » malware, mais il devait prouver qu'il était possible de verrouiller le produit et de réclamer une rançon pour en retrouver les fonctionnalités.

Pas de contrôle sur le type de fichier lu

Comme indiqué à Motherboard, ils ont profité d'un bug dans la gestion des fichiers. Le thermostat, disposant d'un grand écran LCD et fonctionnant sous Linux, accepte en effet les cartes SD pour pouvoir personnaliser par exemple le fond d'écran. Malheureusement, l'appareil ne prête pas une grande attention aux fichiers qui sont stockés et ne mène pas certains contrôles de sécurité. Ils ont donc caché leur malware dans une application présentée sous forme d'image, que le thermostat lit alors puis exécute.

Le résultat, on le connait : le malware prend le contrôle du thermostat, affichant un message à l'utilisateur. Ce dernier se voit réclamer un bitcoin (environ 540 euros actuellement) pour retrouver

l'accès à son appareil connecté. L'attaque n'est pas distante et requiert l'utilisation d'une carte SD, mais il n'est pas complexe de mettre en place des sites malveillants donnant accès à des fichiers vérolés. L'utilisateur télécharge ce qu'il pense être un fond d'écran, le copie sur sa carte SD et insère cette dernière dans le thermostat. Celui-ci se retrouve alors piégé par un ransomware. Le cas est particulièrement courant avec Android, et on l'a encore vu récemment avec des fichiers APK de Pokemon Go, modifiés pour intégrer des malwares.

Comment gérer de pareils cas ?

Pour les chercheurs, l'objectif était surtout de tirer la sonnette d'alarme. « *Nous n'avons aucun contrôle sur nos appareils, et nous ne savons pas vraiment ce qu'ils font, ni comment ils le font* » indique Andrew Tierney, avant d'exposer le fond du problème : « *S'ils commencent à faire quelque chose que vous ne comprenez pas, vous n'avez pas vraiment de moyen de le gérer* ».

Tierney et Munro n'ont pas souhaité préciser le modèle exact du thermostat. Ils ont indiqué à Motherboard qu'ils n'avaient pas pu encore joindre le constructeur pour le prévenir de cette faille, d'autant que le correctif serait simple à développer et à diffuser. Mais ils rappellent dans tous les cas que tout objet connecté installé dans un domicile est un nouveau point d'entrée dans le réseau Wi-Fi de la maison.

Il ne s'agit là que d'un des nombreux vecteurs d'attaque qui peuvent cibler les objets connectés. Dans d'autres cas, ce sont les transmissions qui manquent de sécurité (parfois même d'une couche de chiffrement), quand ce n'est pas une panne des serveurs qui empêche de les utiliser correctement. Les exemples ont tendance à se multiplier et il serait bon que les constructeurs réagissent rapidement.

Publiée le 08/08/2016 à 15:00