Boom de l'IoT : quels enjeux pour la sécurité ?

Si l'IoT a enregistré une croissance exponentielle ces dernières années, on observe également une augmentation alarmante des attaques qui les ciblent. La raison tient au fait que la majorité des objets connectés contient peu, voire aucune mesure de sécurité pour se protéger contre ces attaques.

Avec plus de 7 milliards d'appareils IoT en circulation, les IoT sont devenus une cible privilégiée pour les cybercriminels. A tel point que le taux de réussite des attaques de logiciels malveillants commence à soulever des questions. À ce jour, l'attaque la plus médiatisée est celle du malware Mirai fin 2016, qui est parvenue à transformer des milliers d'appareils IoT basés sur Linux en une armée de botnets qui a ensuite été utilisée pour lancer une série d'attaques DdoS (Distributed Denial of Service, déni de service distribué). Plus récemment, des experts en cybersécurité ont découvert une quantité croissante de logiciels malveillants utilisés pour miner de la crypto monnaie montrant que les cybercriminels explorent différentes possibilités d'exploiter les appareils IoT à des fins lucratives.

La sécurité bien souvent négligée

Avec l'explosion de la popularité de l'IoT, les fabricants et les vendeurs ont accéléré la commercialisation de nouveaux produits et inondé le marché. Malheureusement, pour beaucoup d'entre eux, la sécurité des appareils se trouvait tout en bas des priorités, et a souvent été traitée comme un détail secondaire. Par conséquent, la grande majorité des appareils IoT aujourd'hui en circulation utilisent des identifiants et mots de passe de connexion par défaut, possèdent des configurations et protocoles non sécurisés et sont notoirement difficiles à mettre à niveau. En résumé, ils sont bien trop faciles à pirater. Vient s'ajouter à cela, l'émergence des piratages de protocoles de bas niveau comme KRACK qui crée de nouveaux moyens de compromettre l'infrastructure de l'IoT et d'injecter ou de manipuler des données. Les conséquences sont graves pour les appareils qui se synchronisent ou reçoivent des messages de contrôle depuis une application Cloud.

Vers une nouvelle forme de logiciels malveillants

La simplicité de la plupart des appareils IoT a forcé les cybercriminels à repenser leur approche. En réalité, en raison de leur nature, très peu d'appareils IoT stockent des quantités importantes de données sensibles. Cela rend donc les attaques traditionnelles par ransomwares obsolètes. C'est pourquoi, l'attention s'est tournée vers la manière dont les logiciels malveillants peuvent être utilisés pour asservir les dispositifs IoT (comme c'était le cas pour Mirai), en bloquer l'accès aux utilisateurs, ou pour empêcher les appareils de remplir leur mission initiale. Cet objectif peut sembler assez inoffensif mais si on pense aux appareils IoT qui sont désormais utilisés en tant que pacemakers ou pour contrôler les doses de médicaments de patients hospitalisés, les conséquences peuvent être dramatiques.

Une prise de conscience nécessaire

Face à cette menace croissante, les fabricants et les vendeurs doivent se réveiller et commencer à mettre en oeuvre des mesures de sécurité plus robustes sur tous les appareils IoT, en se

concentrant sur trois domaines essentiels :

Adoption des normes de sécurité logicielle modernes : tout nouvel appareil arrivant sur le marché doit adhérer strictement aux pratiques de sécurité actuelles, comme la protection intégrée des mots de passe qui force les utilisateurs à changer le mot de passe par défaut après achat. Les nouveaux appareils doivent également inclure une assistance logicielle après-vente et la possibilité d'appliquer des correctifs ou des mises à niveau à distance si nécessaire, assurant la durabilité de la sécurité contre de nouvelles formes de logiciels malveillants.

Construction d'un matériel robuste et inviolable : la sécurité physique est aussi une préoccupation essentielle pour les nouveaux appareils. Des choses simples, comme l'ajout d'interrupteurs permettant aux utilisateurs de désactiver des fonctions non utilisées (par exemple un bouton pour désactiver le micro et prévenir contre l'écoute illicite). L'intégration de mesures d'inviolabilité lors de la conception du matériel est également une garantie pour empêcher quiconque ayant un accès direct à l'appareil de le compromettre ou de décoder ses informations sans autorisation.

Utilisation de protocoles réseau sécurisés : des protocoles sécurisés comme HTTPS doivent être mis en place pour tout échange de données entre les appareils IoT et la gestion en backend ou les solutions de stockage. Il est également nécessaire d'utiliser des méthodes d'authentification robustes pour empêcher tout accès frauduleux.

Pendant de trop nombreuses années, les vendeurs et fabricants d'appareils IoT ont ignoré les conventions de sécurité dans leur empressement à commercialiser de nouveaux produits. La multiplication des logiciels malveillants cherchant à exploiter ces vulnérabilités est le résultat direct de ces décisions. Malheureusement, ce sont les clients qui en pâtissent. Bien qu'il soit impossible de revenir en arrière pour améliorer la sécurité des millions d'appareils IoT déjà en circulation, une meilleure mise en oeuvre des pratiques de sécurité sur les nouveaux appareils contribuera considérablement à réduire l'ampleur du problème. Au fur et à mesure que les anciens appareils moins sécurisés atteindront la fin de leur cycle de vie, nous devrions voir la sécurité de l'IoT s'améliorer de façon globale.