Devenons aussi intelligents que les assistants personnels !

Les assistants personnels intelligents, tels que Google Home ou Alexa d'Amazon, sont de plus en plus utilisés par les particuliers, pour se réveiller à l'heure pour aller travailler, pour écouter de la musique, ou encore pour faire des achats en ligne. Ils comportent pourtant de graves failles de sécurité, comme le rappelle Martin Hron, Security Researcher, chez Avast.

Temps de lecture : minute

---

13 mars 2018

Bien que pratiques, les assistants personnels vocaux sont une cible très attrayante pour les cybercriminels au regard de la quantité massive de données sensibles qu'ils détiennent. Ils seront donc tôt ou tard dans le viseur des hackers, ce n'est plus qu'une question de temps. De plus, leurs paramètres de sécurité par défaut sont généralement faibles car ils ont été conçus pour être très simples à utiliser. Ainsi, la configuration initiale présente l'avantage de ne prendre que quelques minutes mais elle comporte des vulnérabilités.

La manière dont les utilisateurs configurent leurs assistants personnels intelligents, et s'en servent ensuite, est cruciale. Beaucoup d'entre eux ne pensent probablement pas à ajuster les paramètres par défaut, soit parce qu'ils ne sont pas conscients des cyber-risques induits, soit parce qu'ils estiment que l'appareil est correctement sécurisé, faisant confiance au constructeur.

Des emails personnels pour tous

La première chose que beaucoup de personnes font lors de l’installation de ces assistants est de les lier à divers comptes, notamment Amazon, Google Mail ou encore Spotify, en utilisant les paramètres par défaut de l'appareil. Cette action, anodine de prime abord, peut néanmoins avoir des conséquences significatives.

Sans une connexion sécurisée, vérifiant que chaque action a bien été ordonnée par le propriétaire du périphérique, ce dernier peut lire des emails à haute voix ou passer une commande, peu importe qui en fait la demande. Cela signifie que tous les membres de la famille, ou toute personne présente dans le foyer, qu’elle soit la bienvenue ou non, disposant d’un assistant personnel intelligent, peut tirer des informations personnelles de l'appareil en question.

À lire aussi
Les assistants vocaux vont-ils signer la mort des écrans ?

Des commandes malveillantes passées à distance

Les cybercriminels n'ont pas nécessairement besoin d'être proches d'un assistant personnel intelligent pour le faire fonctionner, ou même le pirater. Ils peuvent en effet hacker un réseau via un routeur vulnérable et, à partir de là, accéder aux autres périphériques qui y sont connectés. En tirant profit des vulnérabilités d’un autre objet connecté capable de lire des enregistrements, ils pourraient même interagir avec un assistant personnel intelligent. Si celui-ci est mal configuré, il fera tout ce que n’importe quel individu lui ordonnera.

De cette manière, des personnes mal intentionnées peuvent accéder physiquement à une maison à l’aide d’une serrure intelligente ; le cambrioleur n’aura qu’à demander à l’assistant, à travers une fenêtre, de déverrouiller la serrure. Autre alternative : il piratera le réseau domestique et ordonnera à un autre appareil de le commander pour ouvrir la porte d'entrée.

Une vulnérabilité inévitable

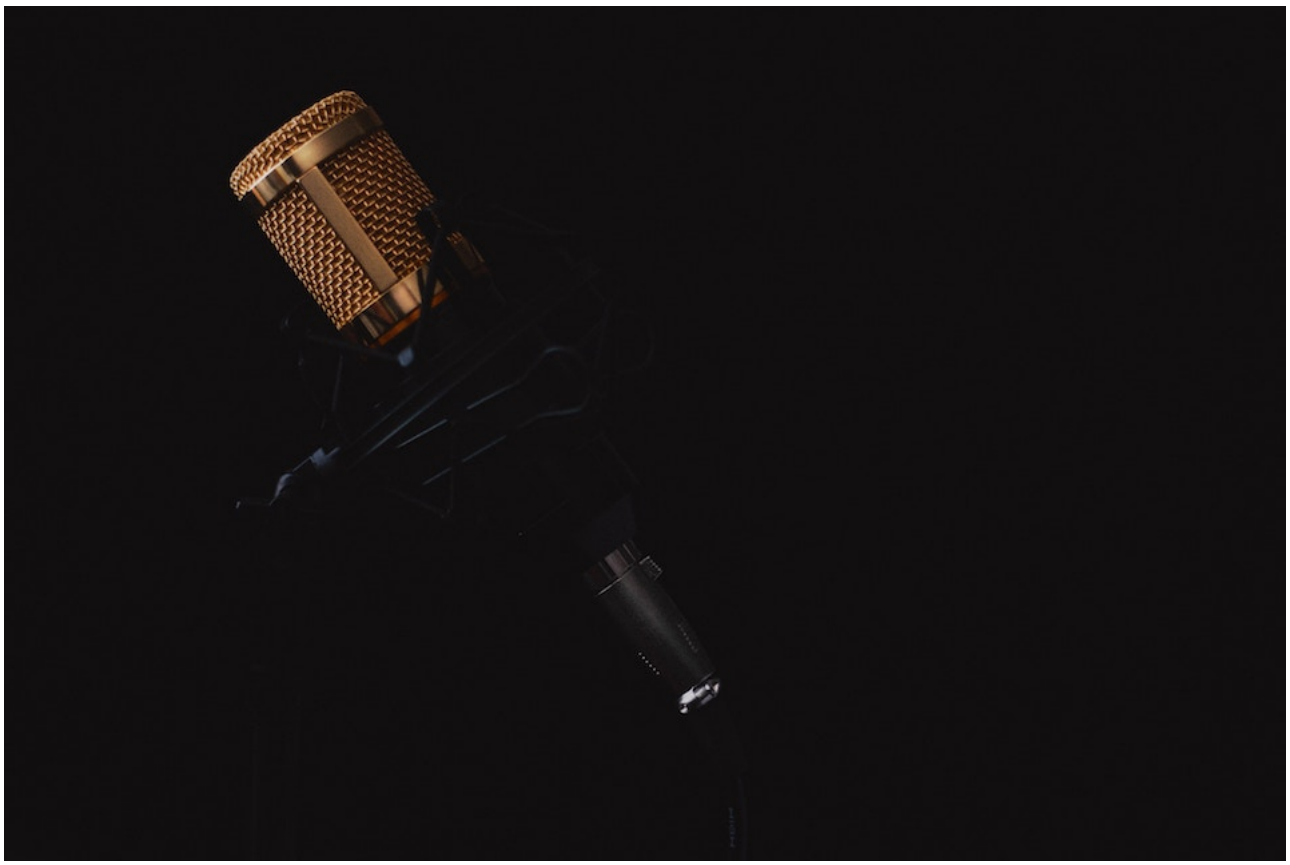
De facto ces objets intelligents sont d’ores et déjà ciblés par des cybercriminels prêts à exploiter des vulnérabilités actuellement inconnues. Par exemple, découverte l'année dernière, la faille BlueBorne permettait à toute personne à proximité d'un appareil compatible Bluetooth, dont Alexa, d’en prendre facilement le contrôle. Le plus souvent, les vulnérabilités sont décelées après plusieurs années, ce qui signifie que des objets connectés de notre quotidien conçus récemment en contiennent potentiellement déjà.

Autre cas, EternalBlue a été découvert des années après sa création accidentelle : développé par la NSA et gardé secret, cet exploit est à

l’origine de WannaCry l’attaque ransomware significative perpétrée en 2017. Il s’agit là du parfait exemple de la manière dont une vulnérabilité peut permettre aux cybercriminels de faire des ravages, avant même d’être connue des professionnels ou du grand public.

Des bonnes pratiques concrètes, de la fabrication à l’utilisation

Pour une protection plus efficace, il est nécessaire que la sécurisation de ces appareils intelligents soit appréhendée dès leur conception, avec des identifiants uniques assignés par les fabricants pour chaque objet manufacturé, et des consommateurs obligés de créer un mot de passe fort – huit caractères minimum et comprenant des lettres, chiffres et signes – lors de la première utilisation.



À lire aussi

6 conseils pour se lancer sur les assistants vocaux

En outre, le réseau Wi-Fi, sur lequel un assistant personnel s’appuie pour fonctionner, doit lui aussi être protégé avec un mot de passe fort, pour faire face à toute tentative de cyberattaques.

Il est important également de mettre à jour l’appareil dès que le fabricant rend un patch disponible. Une bonne pratique qui doit s’accompagner d’une solution de sécurité afin de pallier une mise à jour tardive ou une vulnérabilité non patchée. Ainsi, ce n’est qu’en adoptant des pratiques de cybersécurité responsables et en protégeant les assistants personnels que nous deviendrons plus intelligents qu’eux !

Une sensibilisation accrue, pour faciliter l'adoption de bons réflexes

Le nombre d’assistants personnels intelligents augmente rapidement, ce qui entraine un risque croissant d'attaques. En effet, plus nous nous entourons d'appareils connectés, plus les cybercriminels seront enclins à les cibler. La sensibilisation aux risques de sécurité de ces terminaux doit par conséquent s’accélérer. Il est important que les utilisateurs soient conscients des menaces auxquelles ils s’exposent, notamment lorsqu'ils gardent les paramètres originaux et n’adoptent pas ces bonnes pratiques.

Il faut garder à l’esprit qu’une vulnérabilité pouvant compromettre un terminal peut être déjà présente mais découverte demain, dans cinq ans ou bien peut-être jamais ! Seul l’avenir nous le dira, mais comme le dit l’adage, "*mieux vaut prévenir que guérir*". L’objectif est donc de toujours connaitre les vulnérabilités éventuelles avant les cybercriminels pour garder une longueur d’avance sur eux. Les assistants personnels intelligents ont été conçus pour faciliter notre quotidien, pas celui des hackers !

Il se passera malheureusement encore du temps avant que nous puissions prédire avec précision les attaques toujours plus sophistiquées et inattendues des pirates informatiques. Outre la sensibilisation, seule une collaboration entre les constructeurs, les spécialistes de la sécurité et les utilisateurs pourra permettre de gagner le combat contre les hackers, et ainsi tirer le meilleur parti de tous les objets intelligents qui nous entourent.

Martin Hron, Security Researcher, chez Avast

Article écrit par Geraldine Russell