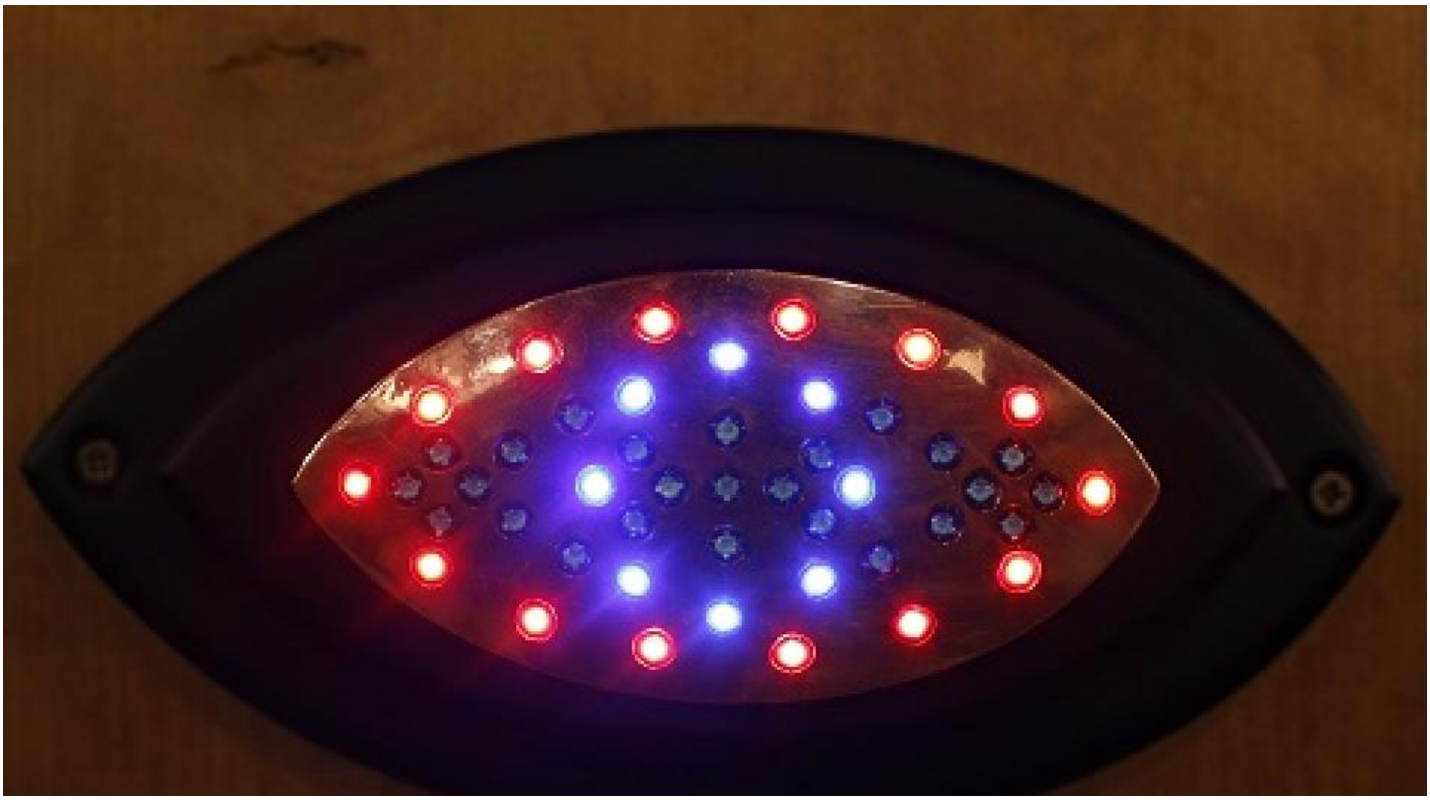
29 mai 2018
Big Amazon

Quand Alexa, l’assistant d’Amazon enregistre ce qui se passe chez vous et l’envoie à d’autres...



Une famille américaine a été victime d'un "bug rarissime" selon Amazon. L'enceinte connectée de la firme, Alexa, a, sans qu'ils ne s'en aperçoivent, enregistré une de leurs conversations et l'a envoyé à un tiers. Prévenus par ce dernier, les protagonistes ont débranché leurs appareils connectés et accusent l'entreprise d'espionnage. De son côté la firme s'est confondue en excuses et a assuré "prendre la confidentialité" très au sérieux.

Avec Frédéric Mouffle

Atlantico : Les médias américains ont pu rapporter l'épisode d'un couple ayant été enregistré à son insu par Alexa, l'assistant vocal d'Amazon, avant que cet enregistrement ne soit envoyé à un contact de leur carnet d'adresse. Une situation qui pourrait s'expliquer, selon Amazon, par une discussion tenue par le couple alors qu'Alexa était activée, et par une compréhension erronée des paroles tenues ayant conduit à l'enregistrement, puis à l'envoi du fichier. Quel est le niveau de vulnérabilité de ces assistants vocaux ? Ce type de cas est-il réellement une exception ?

Frédéric Mouffle : Ce type de cas n’est sans doute pas une exception. Et si cela a pu se produite une fois, nous pouvons raisonnablement penser que cet incident s’est peut-être déjà produit avec ce modèle d’assistant vocal. En 2017, des chercheurs avaient pointé du doigt une faille qui avait pu être découverte, basée sur l’émission de signaux audio basses fréquences, inaudible par l’homme mais perçue par le micro de ces assistants vocaux. Permettant en outre d’envoyer des commandes vocales à l’insu des propriétaires, de passer des appels téléphoniques via *« SIRI »,* et de commander des produits sur Amazon avec *« Alexa ».* Tous les assistants vocaux tels *« SIRI »* ou *« Google assistant »*, sont en définitive concernés par cette faille, dite aussi « faille du dauphin ». Cette expression faisant référence au mode de communication très spécifique de ces mammifères marins basé sur l’usage des basses fréquences. Un journaliste avait d’ailleurs mis en évidence le fait que sa *« Google home »* enregistrait en permanence et transmettait tout aux serveurs Google sans le consentement de l’utilisateur. Google avait alors admis un bug dans son dispositif…

Quels sont les autres risques encourus par les utilisateurs de ce type d'assistants vocaux ? Quels sont les autres appareils (webcams, autres objets à commande vocale…), qui pourraient également nous enregistrer à notre insu ?

Les objets connectés - ou *« IoT »* - représentent un large spectre de vulnérabilités. Il est nécessaire de partir du principe que tous les appareils disposant de micro ou de camera, ou tout autre appareil connectés notamment dans le domaine de la domotique (pèse personne, enceintes, petit électroménager, et autres systèmes de gestion « intelligente » des équipements de la maison), sont potentiellement des sources de captation d’informations clandestines…

Quelques règles simples permettent de limiter ce risque. A savoir : mettre hors tension ses appareils lorsqu'ils ne sont pas utilisés, vérifier que les codes d'accès à ces périphériques ont bien été modifiés par l'utilisateur, vérifier aussi les mises à jour des périphériques car celles-ci permettent, pour certaines d'entre elles de combler des failles de sécurité identifiées par la communauté des spécialistes avertis, ou par les fabricants eux-mêmes.

Comment les utilisateurs peuvent se protéger efficacement contre ces "erreurs" ?

Les utilisateurs doivent consentir à un certain recul par rapport à l'utilisation de ces dispositifs technologiques potentiellement intrusifs. Les assistants vocaux pour la maison, selon moi n'apportent aucune valeur ajoutée réelle. C'est un besoin qui est créé de toute pièce par les géants du web, afin de valoriser artificiellement un peu plus le prix de votre « fiche data ». Et ceci, en exploitant un peu plus vos données personnelles à l'intérieur de votre foyer. Grâce aux navigateurs, ils peuvent savoir ce que vous consultez en matière de sites internet, connaitre vos habitudes de consommation courante sur le Web, identifier vos centres d'intérêt, cibler le type d'actualité que vous consultez quotidiennement, etc… Grâce aux réseaux sociaux, ils identifient vos amis et ciblent vos familles, vos lieux de vacances, et toute une myriade de choses très personnelles… Les téléphones mobiles quant à eux permettent d'affiner votre profil, via la captation de vos données de géolocalisation, le type d'application que vous utilisez. Que cela soit des jeux ou des applications bancaires. C'était au demeurant le chaînon manquant, autrement dit : capter de l'information qui ne passe par aucun réseau de communication habituel.