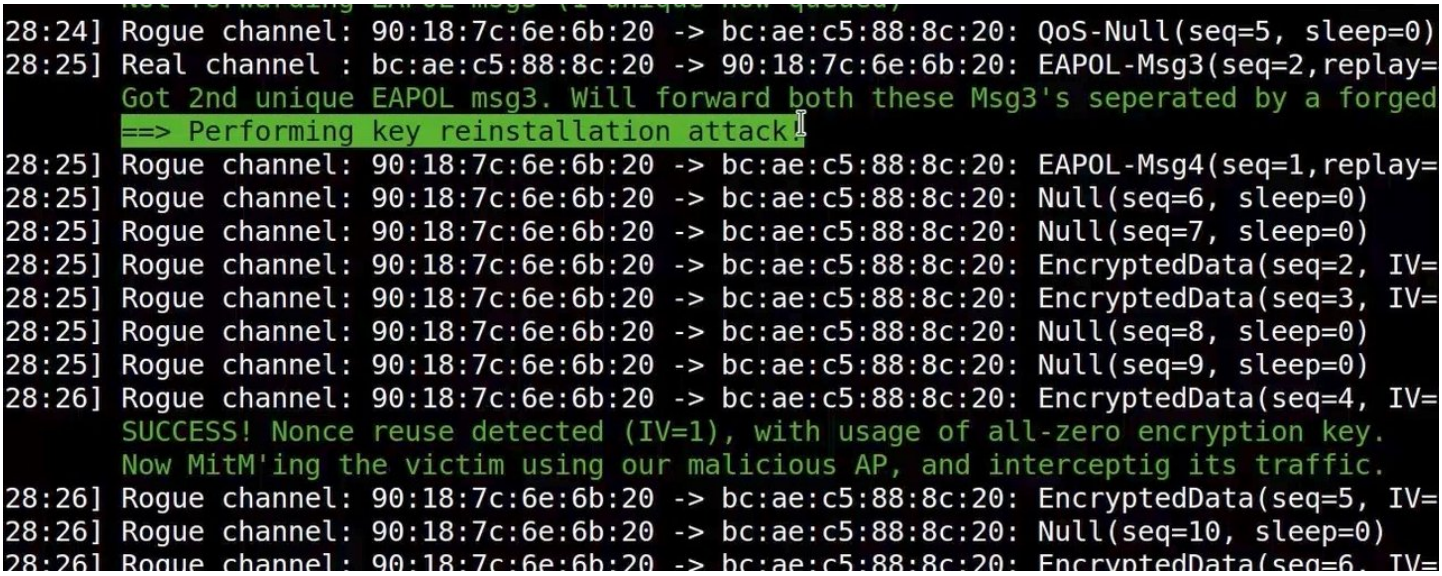

Un extrait de la démonstration effectuée par le chercheur belge.
© DR

TECHNOLOGIE

Tous les Suisses sont concernés par la faille détectée dans le wi-fi

Smartphones, ordinateurs, babyphones ou encore modems sont susceptibles d'être piratés via une nouvelle vulnérabilité. Swisscom, UPC ou encore Sunrise sont sous pression pour mettre à jour leurs appareils.

3 minutes de lecture

Technologies **sécurité**

Anouch Seydtaghia

Publié mardi 17 octobre 2017 à 17:18, modifié mardi 17 octobre 2017 à 17:50.

Depuis dix ans, c'était le système de chiffrement réputé le plus sûr pour sécuriser les réseaux wi-fi. Mais depuis quelques heures, cette certitude s'est envolée. Depuis l'annonce, lundi après-midi, de la découverte d'une faille dans le protocole de chiffrement WPA2, c'est une course contre la montre qui a démarré pour mettre à jour tous les appareils connectés à Internet. En Suisse, Swisscom, Sunrise ou UPC sont concernés.

Lire aussi: Une faille rend les réseaux wifi piratables

Cette alerte mondiale a été lancée par un homme, Mathy Vanhoef. Ce chercheur de l'Université de Louvain en Belgique a démontré en détail sur son site mis en ligne pour l'occasion (krackattacks.com) comment le WPA2 peut être piraté. Les «krack attacks» (pour «key reinstallation attacks», ou «attaques réinstallant une clé») sont capables de déchiffrer le contenu envoyé, de voir tous les sites qui sont consultés via un réseau et d'intercepter les flux de données non sécurisés. Ce ne sont pas seulement les modems et les routeurs qu'il faut, du coup, mettre à jour: smartphones, tablettes, ordinateurs et tous les objets connectés à Internet doivent désormais être sécurisés.

cks: Bypassing WPA2 against Android and Linux

Swisscom répond

Ainsi, tous les internautes suisses et tous les fabricants sont concernés. «C'est la chaîne tout entière qui est responsable. Les utilisateurs doivent mettre la pression sur Swisscom et Swisscom doit mettre la pression sur son constructeur de modems. Ce dernier doit mettre à jour ses appareils, envoyer la mise à jour à Swisscom, qui va devoir la tester puis la déployer pour tous ses utilisateurs», explique Steven Meyer, directeur de la société de sécurité ZENData, à Genève.

Contactés, les opérateurs disent réagir. «Nous analysons actuellement, en collaboration avec les fabricants, quels appareils proposés doivent être mis à jour», explique Swisscom, qui précise ne disposer pour l'heure d'«aucune indication d'avoir été touchée par cette faille». «Nos experts en sécurité des données, tant au niveau de Liberty Global que d'UPC, procèdent actuellement à une analyse détaillée du problème afin d'en mesurer l'importance», explique de son côté le câblo-opérateur. Sunrise est pour sa part «en contact étroit avec les autorités et les fabricants pour définir les mesures nécessaires et corriger rapidement cette faille».

Lire aussi: Un algorithme pour désengorger le réseau wi-fi

«Une décennie»

Aux opérateurs suisses de jouer. Mais pas seulement. «Le vrai problème concerne les appareils wi-fi du type IoT (Internet des objets): est-ce que votre webcam, TV ou fer à repasser connecté va être mis à jour? Probablement pas. Et donc nous sommes partis pour une vulnérabilité qui pourra être exploitée probablement pendant une décennie», avance Steven Meyer. Microsoft a commencé à fournir des correctifs pour Windows et Apple mettra à jour ses iPhone d'ici à quelques jours. La tâche s'annonce plus difficile pour Google et les deux milliards d'utilisateurs de son système Android: il faudra des mois avant que la multinationale ne puisse mettre à jour tous ces appareils.

Il est conseillé aux internautes d'être prudents ces prochaines semaines. Il est inutile de changer le mot de passe de leur wi-fi domestique. Et il est préférable, avec son smartphone ou son ordinateur, de ne consulter que des sites dont l'adresse commence par «https». Sinon, il faut privilégier les connexions en 3G ou en 4G. A noter qu'une attaque ne peut se faire que si le pirate se trouve à proximité d'un appareil vulnérable. Que doivent faire les entreprises? «Nous leur recommandons de mieux contrôler les accès physiques à leur bureau. Elles peuvent aussi enlever leur infrastructure critique du réseau connecté au wi-fi et utiliser un VPN pour ajouter une sous-couche sécurisée dans la communication, afin de crypter les communications avec un autre protocole», conseille Steven Meyer.

À propos de l'auteur

Anouch Seydtaghia
@Anouch

Journaliste éco/finance, spécialisé dans les nouvelles technologies, intéressé par les voitures autonomes, la cybersécurité et les start-up