

Alerte : Faille Wifi du WPA2. Risques et solutions pour s'en protéger



Dévoilée au public lundi 16 octobre 2017, Krack Attacks est une faille qui permet aux pirates d'espionner votre connexion wifi. Que doit-on craindre ? Comment se protéger ? Denis JACOPINI nous apporte des éléments de réponse.

Que doit-on craindre de cette faille découverte dans le WPA2 ?

Mathy Vanhoef, chercheur à l'université KU Leuven, a découvert une faille permettant d'intercepter des données transmises sur un réseau Wi-Fi, même lorsqu'il est protégé par le protocole WPA2. Pire, il est également possible d'injecter des données, et donc des malwares, en utilisant la technique découverte. Les réseaux domestiques aussi bien que les réseaux d'entreprises sont concernés, c'est donc une découverte majeure dans le domaine de la sécurité informatique.

La technique décrite par Mathy Vanhoef est appelée Key Reinstallation Attack, ce qui donne KRACK.

Comment se protéger de cette faille ?

Il n'y a pas de meilleur protocole que le WPA2. Il ne faut surtout pas revenir au protocole WEP. Changer de mot de passe ne sert à rien non plus. Le seul moyen de se protéger de cette faille est de mettre à jour votre système d'exploitation et les appareils concernés. Les acteurs du marché, fabricants ou éditeurs, ont été notifiés de cette faille le 14 juillet 2017. Certains l'ont comblée par avance comme Windows.

Il faut combler la faille à la fois sur les points d'accès et sur les clients, c'est-à-dire que patcher vos ordinateurs et smartphones ne vous dispense pas de mettre à jour votre routeur ou votre box Wi-Fi.

Même si, en tant qu'utilisateur, vous n'avez pas grand chose à faire de plus que de mettre à jour votre système d'exploitation et le firmware de votre point d'accès pour vous protéger contre la faille Krack Attacks, nous vous énumérons une liste de préconisations qui mises bout à bout, rendront plus difficile aux pirates les plus répandus l'intrusion dans votre Wifi.

Les Conseils de Denis JACOPINI pour avoir un Wifi le plus protégé possible :

1. Mettez à jour les systèmes d'exploitation de vos ordinateurs, smartphones, tablettes et objets.
2. Mettez à jour votre point d'accès Wifi (le firmware de votre Box, routeur...)
3. Modifier le SSID ;
4. Modifier le mot de passe par défaut ;
5. Filtrage des adresses MAC (facultatif car peu efficace);
6. Désactiver DHCP ;
7. Désactiver le MultiCast (pour les appareils qui disposent de cette fonction) ;
8. Désactiver le broadcast SSID (pour les appareils qui disposent de cette fonction) ;
9. Désactiver le WPS (pour les appareils qui disposent de cette fonction) ;
10. Utilisez un VPN ou un accès https pour envoyer ou recevoir des informations confidentielles
11. Choisissez un cryptage fort de votre Clé WIFI :
 - Technologie WPA 2 (également connu sous le nom IEEE 802.11i-2004) ;
 - **Protocole de chiffrement AES** (ou CCMP) : **Important !**

Des personnes peuvent accéder librement à votre Wifi ?

Condition exigée depuis plusieurs années par les touristes et les nomades, il y a de fortes chances que les clients de votre hôtel, de vos chambres d'hôtes, de vos gîtes ou tout simplement des amis vous demandent absolument de disposer du Wifi.

Je tiens à vous rappeler que selon l'article L335-12 du Code de la Propriété Intellectuelle, l'abonné Internet reste le seul responsable des usages de sa connexion.

Ainsi, je ne peux que vous conseiller d'être prudent concernant l'usage de votre connexion Wifi par des tiers et de vous munir de moyens technologiques permettant de conserver une trace de chaque personne se connectant sur votre Wifi afin que si votre responsabilité en tant qu'abonné à Internet était recherchée, vous pourriez non seulement vous disculper mais également fournir tous les éléments permettant l'identification de l'individu fraudeur.

Les personnes intéressées par les détails techniques, et pointus, concernant la découverte de la faille WPA2 peuvent se rendre sur le site du chercheur dédié à ce sujet.

Bulletin d'alerte du CERT-FR

Va-t-on aller vers un WPA 3 ?

LE NET EXPERT

:

- SENSIBILISATION / FORMATIONS :
 - CYBERCRIMINALITÉ
- PROTECTION DES DONNÉES PERSONNELLES
 - AU RGPD
 - À LA FONCTION DE DPO
- MISE EN CONFORMITÉ RGPD / CNIL
 - ÉTAT DES LIEUX RGPD de vos traitements
 - MISE EN CONFORMITÉ RGPD de vos traitements
 - SUIVI de l'évolution de vos traitements
- RECHERCHE DE PREUVES (outils Gendarmerie/Police)
 - ORDINATEURS (Photos / E-mails / Fichiers)
 - TÉLÉPHONES (récupération de Photos / SMS)
 - SYSTÈMES NUMÉRIQUES
- EXPERTISES & AUDITS (certifié ISO 27005)
 - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
 - SÉCURITÉ INFORMATIQUE
 - SYSTÈMES DE VOTES ÉLECTRONIQUES

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Réagissez à cet article

Source : *KRACK Attacks: Breaking WPA2 / KRACK : faille du Wi-Fi WPA2, quels appareils sont touchés ? Comment se protéger ?*