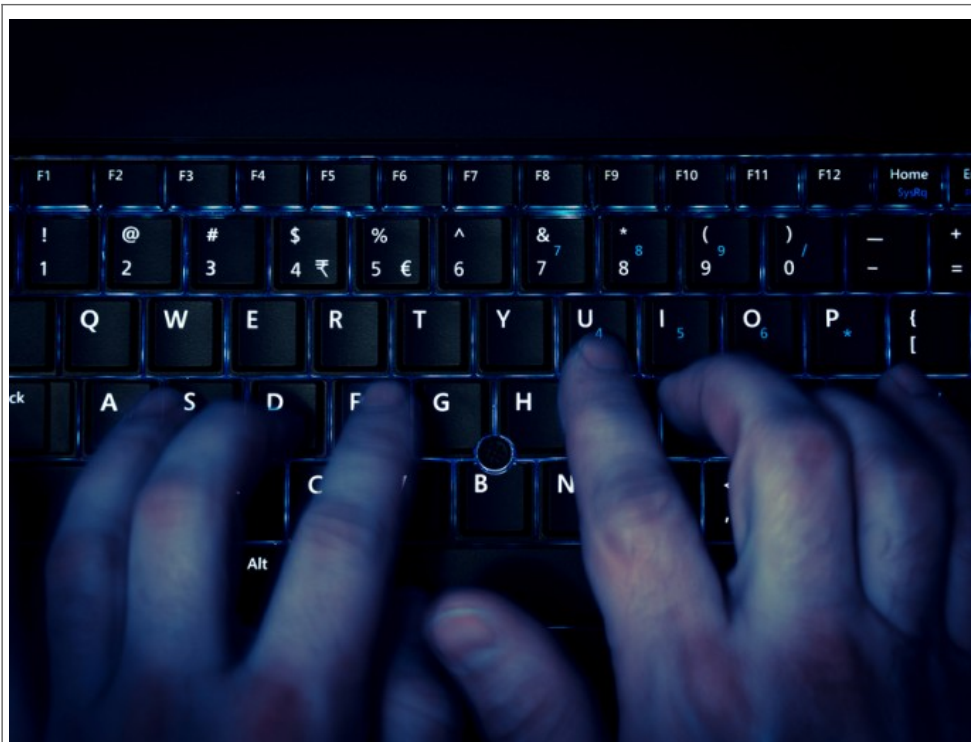


Les claviers sans fil pourraient aussi servir à espionner !



Les
claviers
sans fil
pourraient
aussi
servir
à espionner
!

Avec un simple dongle USB, une antenne et quelques lignes de code, un pirate peut capter toutes les frappes d'un clavier sans fil, selon la start-up Bastille.

Après les souris (MouseJack), les claviers sans fil... Avec une simple antenne et un dongle USB, plus quelques lignes de code écrites en Python, un pirate peut enregistrer « toutes » les frappes réalisées par l'utilisateur d'un clavier sans fil bon marché ou générer ses propres frappes, selon la start-up américaine Bastille. Et ce dans un rayon de plusieurs dizaines de mètres autour de la cible.

Claviers sans fil vulnérables

« Lorsque nous achetons un clavier sans fil, nous nous attendons à ce que le fabricant ait conçu et intégré la sécurité nécessaire au cœur du produit », a déclaré Marc Newlin, ingénieur et chercheur chez Bastille. « Nous avons testé les claviers de 12 fabricants et nous avons constaté, malheureusement, que 8 d'entre eux (soit les deux tiers) sont vulnérables à une attaque [que l'on nomme] KeySniffer ».

Ces claviers sans fil utilisent le plus souvent des protocoles radio propriétaires peu testés et non sécurisés pour se connecter à un PC, à la différence du standard de communication Bluetooth. Ils sont d'autant plus faciles à détecter car leur signal est toujours actif... Les fabricants concernés (dont HP, Toshiba et Kensington) ont tous été alertés. Selon Bastille, la plupart, voire tous les claviers exposés à KeySniffer ne peuvent pas être mis à jour et devront être remplacés.

Absence de chiffrement

En 2010 déjà, les développeurs de DreamLab Technologies ont exposé une faille dans un clavier sans fil Microsoft. Le « renifleur » et programme Open Source KeyKeriki a capté le signal et déchiffrer les données transmises à un ordinateur... Mais la découverte de Bastille, KeySniffer, est différente. Elle montre que des fabricants produisent et vendent encore des claviers wireless sans chiffrement.

La start-up recommande aux internautes d'utiliser un clavier filaire pour se protéger.

Article original de Ariane Beky



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Les claviers sans fil, des espions en puissance