

# Comment pirater des codes PIN en sniffant le WiFi des smartphones ?



Comment  
pirater des  
codes PIN  
en sniffant  
le WiFi des  
smartphones  
?

**Des chercheurs peuvent récupérer des données sensibles en se basant sur les perturbations du signal WiFi lors des frappes sur l'écran.**

Quand un utilisateur déplace ses doigts sur l'écran tactile de son téléphone, il perturbe le signal WiFi émis par son terminal. Ces interruptions peuvent être interceptées par un pirate, analysées et en appliquant de la rétro-ingénierie deviner quelle sont les frappes saisies sur le téléphone ou dans les champs de saisie de mot de passe.

Ce type d'attaque est nommé WindTalker (messenger du vent), par des chercheurs chinois et elle n'est possible que si le pirate contrôle le point d'accès WiFi (un hotspot par exemple dans un rayon de 1,5 mètre) afin de collecter les perturbations du signal WiFi. Un contrôle impératif pour analyser le trafic et savoir quand l'utilisateur accède à des pages nécessitant une authentification.

## **Le CSI en ligne de mire**

Si l'attaque semble issue du domaine de la science-fiction, cette menace se sert du CSI (Channel State Information), un composant du protocole WiFi chargé de fournir les informations générales sur l'état du signal WiFi. Quand l'utilisateur tape du texte sur l'écran, sa main modifie les propriétés de CSI du signal WiFi sortant et la modification peut être captée par un point d'accès malveillant.

Dans une démonstration exposée lors de la ACM Conference on Computer and Communications Security à Vienne, les chercheurs ont montré qu'en réalisant une analyse et un traitement basique du signal, un pirate peut avoir accès aux signaux CSI perturbés et deviner avec une précision moyenne de 68,3% les caractères qu'un utilisateur a tapé. La précision de WindTalker est différente selon les modèles de smartphones et elle peut être améliorée avec le niveau de données collectées...[lire la suite]

---

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



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 : WindTalker : pirater des

codes PIN en sniffant le WiFi des smartphones