# Examen et recommandations pour AirSnitch

## Table des matières

## Introduction

Ce document décrit une révision du livre blanc d'Airsnitch, avec des recommandations et des actions possibles. Elle s'applique aux déploiements sur site et dans le cloud

## Résumé

Le 26 février 2026, des chercheurs ont publié un article intitulé « AirSnitch : Démystifier et briser l'isolement client dans les réseaux Wi-Fi. » Dans cet article, les chercheurs ont présenté des méthodes permettant de contourner des implémentations spécifiques à un fournisseur de protections d'isolation de client de monodiffusion pour des clients sans fil dans le même SSID. Il convient de noter que les attaques d'isolement de client proposées sont des « attaques internes (malveillantes internes) » qui exigent que le pirate soit associé et authentifié à l'infrastructure sans fil avant de lancer l'attaque. Ces méthodes de contournement ne sont pas dues à des vulnérabilités dans les spécifications ou les produits sans fil. Les méthodes de cryptage du réseau sans fil ne présentent pas non plus de vulnérabilité. Ces attaques sont considérées comme opportunistes et risquent d'échouer dans un réseau d'entreprise déployé avec une sécurité multicouche basée sur les meilleures pratiques pour le sans fil, la commutation et le routage.

L'objectif principal des attaques AirSnitch est d'atteindre une position Machine-in-the-Middle (MitM), permettant à un attaquant d'intercepter, de lire et de modifier le trafic entre un client victime et Internet, même lorsque l'isolation du client est activée. L'étude classe ces contournements en trois couches :

- Abus de clé partagée : exploitation du fait que les clés de diffusion/multidiffusion (GTK) sont partagées entre tous les clients d'un ensemble de services de base sur un point d'accès.
- Attaques par injection au niveau de la couche de routage (Gateway Bouncing) : exploitation de l’injection ARP/compromission des adresses MAC au niveau de la couche réseau/IP.
- Couche de commutation (vol de port) : exploitation du comportement d’apprentissage MAC interne des points d’accès et des commutateurs.

Dans le contexte d'un point d'accès client/SOHO, toutes les fonctionnalités sont généralement exécutées au sein d'un seul périphérique (point d'accès sans fil, commutateur et routeur de couche 3), ce qui laisse les périphériques susceptibles d'être mal configurés ou mal isolés entre les couches. Pour l'entreprise, chaque fournisseur dispose d'une conception de réseau basée sur les meilleures pratiques afin de permettre la segmentation et l'isolation à l'aide des principes de confiance zéro au sein de chaque couche du réseau.

À noter également : aucune console de journalisation/d'alarme ou de gestion n'a été utilisée dans

le scénario d'entreprise où les alarmes classiques, telles que la détection des adresses MAC ou IP en double, étaient activées, ce que la plupart des périphériques d'entreprise modernes signalent et consignent.

Cela implique que ces attaques internes, en particulier dans le scénario d'entreprise, ont été lancées dans un réseau non géré/non surveillé ou dans un réseau où la télémétrie n'a pas été configurée pour être livrée à une console de sécurité (logiciel Security Incident and Event Monitoring).

## Produits concernés

Les attaques décrites dans le document sur les points d'accès d'entreprise peuvent être efficaces lorsqu'elles sont utilisées avec des produits de points d'accès sans fil Cisco et des produits sans fil Cisco Meraki (MR), où aucune configuration de sécurité supplémentaire basée sur les meilleures pratiques n'est déployée sur les points d'accès, les contrôleurs sans fil, la commutation et l'infrastructure de routage.

## Recommandations

Pour réduire les risques d'attaques présentés dans ce document, Cisco recommande d'utiliser les meilleures pratiques de défense en profondeur dans chaque couche du réseau. Voici des conseils généraux et un résumé des meilleures pratiques :

- Abus de clé partagée : l'abus de clés partagées (monodiffusion ou groupe) est largement connu depuis que les vulnérabilités ont été révélées avec WPA2-Personal. Même avec l'avènement du WPA3-Personal, le concept de clés partagées entraîne une fuite de la clé (distribution, partage entre les périphériques, ingénierie sociale) compromettant non seulement le SSID mais l'ensemble du réseau de l'entreprise en permettant l'accès à l'infrastructure réseau. Si vous déployez une mise en réseau basée sur des phrases de passe dans l'entreprise, vous devez surveiller et profiler avec soin les périphériques connectés au réseau. Une fois que la phrase de passe/le mot de passe est transmis à un initié malveillant, il est trivial de mettre en place un « point d'accès non autorisé » pour lancer une attaque de type « Machine-in-the-Middle ». Les réseaux à clés partagées (WPA2/WPA3-Personal) ne doivent pas être considérés comme « sécurisés par l'entreprise », à moins que des mesures actives soient prises pour comprendre les périphériques sur le réseau et utiliser d'autres technologies de segmentation (VLAN, VRF, fabrics, pare-feu, etc.) ainsi qu'une rotation fréquente de la phrase de passe.

En ce qui concerne l'utilisation abusive de l'IGTK partagé, la télémétrie au sein d'un réseau sans fil d'entreprise peut émettre une alerte en fonction de la présence d'un message de veille WNM utilisant l'IGTK partagé.

Cisco recommande également de mettre en oeuvre la sécurité de la couche transport pour chiffrer les données en transit dans la mesure du possible, car cela rendrait les données acquises inutilisables par l'agresseur.

- Attaques par injection au niveau de la couche de routage (Gateway Bouncing) et vol de port

de couche 2 : l'hypothèse de cette attaque est qu'un interne malveillant est autorisé à router des paquets de couche 3 (ou à affecter la table ARP d'autres périphériques au sein du BSS). Plus précisément, « nous constatons qu'un pirate peut envoyer des paquets de données dont l'adresse IP de destination est celle de la victime et l'adresse MAC de destination est celle de la passerelle du réseau ». Il existe plusieurs mécanismes au sein de l'infrastructure réseau d'entreprise qui permettraient d'atténuer et d'alerter ce type d'activité malveillante. Les fonctionnalités de couche 2 et de couche 3 recommandées au sein de l'entreprise sont les suivantes :

- Surveillance DHCP : ceci empêche un pirate d'usurper un serveur DHCP et aide à construire une table de liaison de paires IP/MAC légitimes.
- Dynamic ARP Inspection (DAI) : utilise la table de liaison de surveillance DHCP pour intercepter et rejeter les paquets ARP avec des liaisons MAC-IP non valides, empêchant ainsi la phase de reconnaissance des attaques MitM.
- Sécurité des ports : limite le nombre d'adresses MAC autorisées sur un seul port physique (la liaison ascendante des points d'accès) pour empêcher un pirate d'inonder le commutateur d'adresses MAC usurpées.
- Listes de contrôle d'accès VLAN (VACL) / Listes de contrôle d'accès de routeur : refusent explicitement le trafic lorsque les adresses IP source et de destination appartiennent au même sous-réseau client. Cela évite le rebondissement de la passerelle en s'assurant que le routeur abandonne le trafic interne en épingle à cheveux.
- IP Source Guard (IPSG) : empêche l'usurpation d'adresse IP en filtrant le trafic en fonction de la base de données de liaison de surveillance DHCP. Si un pirate tente d'envoyer un paquet avec l'adresse IP utilisée par la victime, le commutateur le dépose sur le port d'entrée.
- Unicast Reverse Path Forwarding (uRPF) : permet de s'assurer que les paquets arrivant sur une interface proviennent d'une adresse source légitime et accessible, réduisant ainsi certaines formes d'usurpation d'adresse IP.

# Conclusion

Les recherches présentées dans le document d'AirSnitch rappellent de manière critique que l'« isolement client » est une caractéristique localisée plutôt qu'une frontière de sécurité complète. Bien que les chercheurs aient réussi à démontrer les contournements en utilisant leurs configurations spécifiques qui pourraient ne pas être alignées sur les meilleures pratiques des fournisseurs, il est important de les classer comme des attaques internes opportunistes qui exploitent un manque de configuration de sécurité entre les couches réseau plutôt que des failles inhérentes dans les protocoles de cryptage sans fil définis dans la norme 802.11 ou la Wi-Fi Alliance.

Pour l'entreprise, le principal point à retenir est que la sécurité ne peut pas s'appuyer sur une seule bascule « marche/arrêt ». Les vulnérabilités identifiées, telles que le rebond de la passerelle et le vol de ports, sont efficacement neutralisées lorsqu'une stratégie de défense en profondeur est appliquée. En abandonnant les environnements à clé partagée (WPA2/3-Personal) au profit de l'authentification basée sur l'identité (WPA3-Enterprise) et en mettant en oeuvre de solides protections de couche 2 et de couche 3, notamment la surveillance DHCP, l'inspection ARP

dynamique (DAI), les listes de contrôle d'accès (VACL) et la segmentation et la classification robustes des périphériques, les entreprises peuvent s'assurer que le trafic client reste isolé même si un pirate obtient un accès authentifié au SSID.

De plus, l'absence de télémétrie de gestion dans les scénarios de test d'entreprise des chercheurs souligne l'importance de la visibilité. Dans un environnement Cisco géré, les comportements anormaux requis pour exécuter ces attaques, tels que les adresses MAC dupliquées, l'usurpation d'adresse IP ou les messages WNM non autorisés, déclencheraient des alertes immédiates dans un système SIEM (Security Incident and Event Management).

## Recommandation Finale

Les clients Cisco doivent revoir leurs déploiements sans fil pour s'assurer qu'ils appliquent les architectures Zero Trust établies. En intégrant la sécurité sans fil aux protections de l'infrastructure filaire et en maintenant une surveillance active, les risques posés par les attaques de type AirStinch sont considérablement réduits, garantissant un environnement réseau sécurisé et résilient.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.