# Attaques de type man-in-the-middle

## Prévention des attaques réseau sur les appareils mobiles

Les données sensibles étant de plus en plus accessibles via les appareils mobiles, les menaces mobiles sont de plus en plus répandues et sophistiquées. Les attaques de type man-in-the-middle sont un exemple éloquent de ces menaces sophistiquées et, selon une récente étude, 24 % des organisations signalent que des appareils mobiles utilisés dans leur entreprise ont été connectés à un réseau Wi-Fi malveillant.[1]

### Fonctionnement d'une attaque de type man-in-the-middle

En général, une attaque de ce type sur des données d'entreprise se déroule en deux temps :

1. Accéder au trafic réseau
2. Déchiffrer les données

La deuxième étape est importante car les données d'entreprise sont presque toujours chiffrées et le simple fait de se placer au milieu du trafic ne signifie pas qu'il y aura vol de données.

#### 1. Accéder au trafic réseau

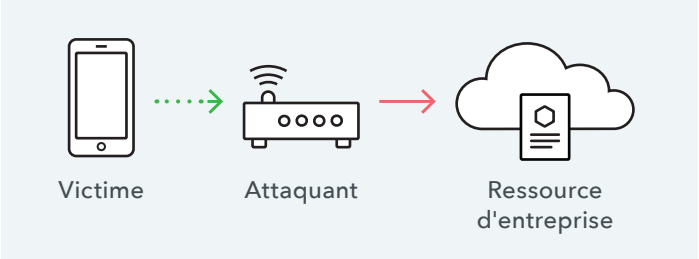
Il existe plusieurs façons pour un attaquant d'accéder au trafic réseau, notamment :

A. Configurer un point d'accès Wi-Fi ou une antenne relais factice

B. Mettre en place un VPN pour faire passer le trafic dans son réseau

C. Implémenter un proxy pour rediriger le trafic vers son chemin réseau

D. Usurper le protocole ARP (Address Resolution Protocol) pour afficher sa propre adresse matérielle plutôt qu'une passerelle




#### 2. Déchiffrer les données

Une fois sur le chemin du réseau, le hacker peut alors manipuler la connexion ou l'utilisateur pour accéder aux données chiffrées. Cette étape suppose en général le recours à l'une des méthodes suivantes :

#### Détournement du certificat de l'hôte

Un attaquant insère une autorité de certification malveillante sous son contrôle dans la liste des autorités de certification racine de l'appareil de la victime pour pouvoir se faire passer pour une ressource d'entreprise avec laquelle la victime entend communiquer de manière sécurisée.

#### SSLStrip

Un attaquant détourne les connexions non chiffrées de la victime, en réécrivant les URL dont le protocole est normalement sécurisé (HTTPS) en texte simple (HTTP).

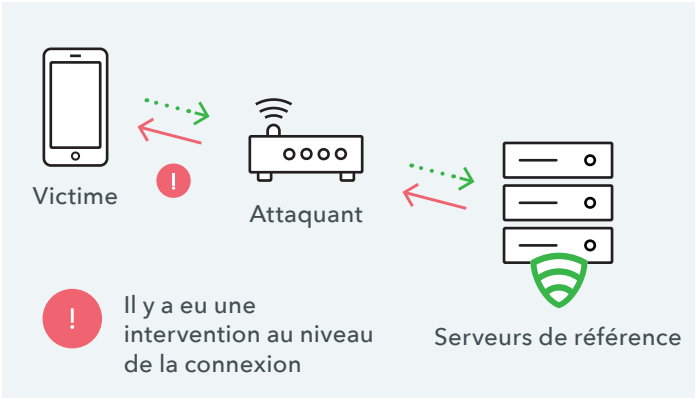
#### Régression de protocole TLS

Un attaquant manipule la connexion négociée pour déclasser le protocole ou chiffrer les suites et ainsi réduire les garanties de sécurité de la connexion.

[1] CIO.com, « One-fifth of IT pros say their companies had mobile data breach » (20 % des professionnels IT déclarent que leur entreprise a subi une fuite de données mobile), 2016

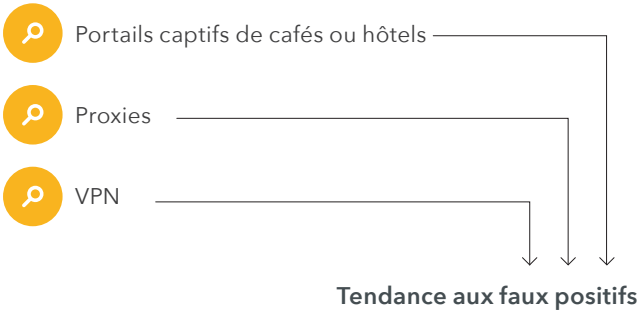
## L'approche de Lookout

Notre application installé sur l'appareil permet de sonder des serveurs de référence aux propriétés de certificat et configurations de protocole de sécurité connues. Cette méthode nous permet de comparer les propriétés de configuration de réseau *attendues* et celles *observées*. En analysant la réponse de ces connexions observées aux propriétés attendues, nous pouvons déterminer si elles sont compromises par un attaquant utilisant l'une des techniques décrites plus haut.

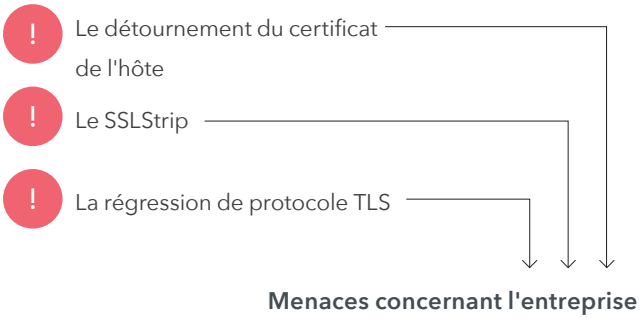



## L'approche de Lookout réduit les faux positifs

**Nous n'alertons PAS UNIQUEMENT sur les :**




**Nous DONNONS L'ALERTE sur :**




L'approche de Lookout se concentre sur les risques les plus pertinents pour les entreprises, à savoir les tentatives d'interception de données chiffrées en transit.

La plupart des programmes de mobilité progressive n'empêchent pas un employé de se connecter aux réseaux Wi-Fi des cafés, hôtels ou aéroports, car cela nuirait à la productivité. Cependant, d'autres approches de détection d'attaques de type man-in-the-middle entraînent des alertes à destination des administrateurs pour ce type d'activité quotidienne. Ces autres approches génèrent de très nombreux faux positifs non exploitables pour la plupart des organisations informatiques.

L'approche de Lookout se concentre sur les types de connexion qui mettent en danger les données chiffrées. Ainsi, nous réduisons le nombre de faux cas positifs de connexion à des réseaux malveillants tout en permettant aux utilisateurs de rester connectés et productifs en déplacement.