Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

# INGERENCE ECONOMIQUE

Flash n° 23 - Avril 2016

Ce « flash » évoque des actions d'ingérence économique dont des sociétés françaises sont régulièrement victimes. Ayant vocation à illustrer la diversité des situations auxquelles les entreprises sont susceptibles d'être confrontées, il est mis à votre disposition pour vous accompagner dans la diffusion d'une culture de sécurité interne.

Vous comprendrez que, par mesure de discrétion, le récit ne comporte aucune mention permettant d'identifier les entreprises visées.

Pour toute question relative à ce « flash » ou si vous souhaitez nous contacter, merci de vous adresser à : securite-economique@interieur.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

Flash n°23 Avril 2016

# Les dangers liés aux Wi-Fi publics

Depuis plusieurs années, la DGSI a connaissance de compromissions informatiques, conséquences d'une utilisation imprudente de Wi-Fi publics.

Voici deux exemples représentatifs des risques liés au faible niveau de sécurité de ce type d'équipement :

## Cas n°1

Le directeur commercial d'une PME française a vu sa messagerie électronique compromise, alors qu'il se rendait à une conférence internationale à l'étranger. A l'arrivée dans le pays de destination, il avait en effet activé la fonction Wi-Fi de son smartphone pour consulter ses courriels professionnels.

Quelques heures plus tard, il recevait des courriels de plusieurs collègues lui signalant qu'il leur avait envoyé des messages inhabituels, écrits en anglais, les invitant à cliquer sur un lien suspect. Il constatait également qu'une partie de sa boîte de réception avait été effacée.

## Cas n°2

« DarkHotel » est un groupe de pirates informatiques, identifié fin 2014 par un éditeur de sécurité informatique, spécialisé dans le piégeage des réseaux Wi-Fi d'hôtels asiatiques dans lesquels séjournent de nombreux cadres d'entreprises en voyage d'affaires.

Le mode opératoire des attaquants consiste notamment à pirater les portails d'identification au réseau Wi-Fi des hôtels. En se connectant, les victimes sont incitées à télécharger des fausses mises à jour pour des logiciels comme Adobe Flash ou des barres d'outils Google. Il s'agit en réalité de maliciels qui vont permettre aux pirates informatiques de prendre le contrôle de la machine de la victime pour exfiltrer de l'information sensible.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

Flash n°23 Avril 2016

## Commentaires

Aujourd'hui, la plupart des lieux publics (restaurants, cafés, aéroports, hôtels, centres commerciaux, gares, etc.) en France et à l'étranger, proposent à leurs clients ou aux simples visiteurs **un accès gratuit à Internet via des réseaux Wi-Fi.**

Dans le cadre de déplacements professionnels mais également personnels, il est alors tentant d'y connecter son smartphone, sa tablette ou son ordinateur portable afin d'accéder à diverses ressources informatiques (messageries électroniques, compte bancaire, réseaux sociaux, extranet, espace de stockage en ligne, etc.).

Malheureusement, ces accès publics sont généralement vulnérables, en raison d'un faible niveau de sécurité.

Des utilisateurs malveillants peuvent notamment **exploiter ces failles pour intercepter les communications** (identifiants de connexion à des messageries électroniques, mots de passe, numéro de carte bancaire, historique de navigation Internet, etc.) transitant par ces points d'accès Wi-Fi.

Il est également très facile pour des pirates informatiques de créer de vrais-faux réseaux Wi-Fi usurpant le nom d'une enseigne reconnue, accessibles gratuitement et sans mot de passe. Cette manœuvre leur permet de récupérer des informations techniques sur les systèmes ainsi que de nombreuses données personnelles et sensibles facilitant de nouvelles intrusions informatiques.

## Préconisations de la DGSI

Afin de réduire les risques de vol de données sensibles d'une connexion à un Wi-Fi public, la DGSI recommande d'appliquer les bonnes pratiques suivantes :

- Privilégier des **connexions cellulaires en 3G/4G**, en France et à l'étranger, pour des usages professionnels ;
- Utiliser **obligatoirement** un VPN en cas d'utilisation d'un point d'accès Wi-Fi public ;
- Désactiver le mode Wi-Fi **quand il n'est pas utilisé** ;
- **Mettre à jour régulièrement** le système d'exploitation, le navigateur Internet (et ses extensions), son antivirus et les logiciels comme Adobe Reader et Flash ;

- **Privilégier les sites Internet sécurisés utilisant du HTTPS** (une extension à installer sur les navigateurs Internet telle que HTTPSANYWHERE permet également d'automatiser le passage de certains sites Internet en HTTPS).

En cas de doute après avoir été connecté à un Wi-Fi public :

- **Changer rapidement les mots de passe des applications** (messageries électroniques, réseaux sociaux, comptes bancaires, espace de stockage en ligne, etc.) que vous utilisez le plus souvent.