Darkhotel : une menace de sécurité IT vraiment évaluée en France ?

Kaspersky Lab a dévoilé cette semaine le fonctionnement des attaques **Darkhotel**, qui ont pour but de dérober des informations sensibles aux cadres supérieurs, pendant leurs voyages d'affaires, via les bornes d'accès Wi-Fi mis à disposition des clients dans les hôtels de luxe.

Les pirates exploitant des failles logicielles à travers les réseaux Wi-Fi "privés et sécurisées" de ce type d'établissements haut de gamme. La zone Asie-Pacifique étant la plus touchée par ce phénomène, estime Kasperky.

On sait que les hotspots installés dans des lieux publics comme les aéroports, les bibliothèques, les bars et les établissements hôteliers nécessitent de prendre des précautions. C'est un souci à la fois de sécurité informatique et économique. Les pouvoirs publics abordent la problématique de l'accès Internet sans fil d'un point de vue général. Mais le cas de Darkhotel est spécifique et semble échapper au radar.

Dans une note de mars 2013 plutôt destinée aux administrateurs de réseaux sans fil, l'ANSSI apporte une vision technique à travers des recommandations de sécurité relatives aux réseaux Wi-Fi.

En se rapprochant des préoccupations des hommes d'affaires, l'agence nationale de sécurité informatique avait néanmoins précisé "qu'en situation de mobilité, lors de toute connexion à des points d'accès Wi-Fi qui ne sont pas de confiance (par exemple à l'hôtel, la gare ou l'aéroport), préalablement à tout échange de données, utiliser systématiquement des moyens de sécurité complémentaires (VPN IPsec par exemple)."

En France, des prestataires de solutions comme Ucopia, qui affichent des références clients dans l'hôtellerie de luxe comme Le Ritz, Hôtel Costes, Hôtel Bedford, Hôtel Château Frontenac, Hôtel Franklin Roosevelt, Splendid Etoile, Hôtel Rochester ou Hôtel du Palais (Biarritz) sont concernés.

Ucopia a d'ailleurs entamé une démarche de certification ANSSI de ses produits. En 2010, elle a obtenu une Certification de Sécurité de Premier Niveau (CSPN) pour sa solution UCOPIA de contrôle d´accès au réseau (version 3.0). Nous attendons des éléments de réponse complémentaires de la part du fournisseur de solutions pour réseaux sans fil.

ANSSI – D2IE : quels angles de vue retenus ?

Plus récemment, l'ANSSI a évoqué les risques de vol d'informations sensibles en cas de déplacements professionnels. Initialement présenté en février 2010 avec la collaboration du Club des Directeurs de Sécurité des Entreprises, le Passeport de conseils aux voyageurs a été mis à jour en septembre.

Ce guide récapitule les menaces qui pèsent sur la circulation de l'information lors des voyages d'affaires et dresse une liste de recommandations pour se prémunir des vols de documents. Mais,

dans cette version updatée, le cas de l'accès Wi-Fi dans les hôtels n'est pas abordé de manière explicite.

Sur la partie consacrée aux précautions à prendre pendant la mission, il est préconisé de ne pas connecter "ses équipements à des postes ou des périphériques informatiques qui ne sont pas de confiance". L'ANSSI pensait davantage à l'utilisation d'une clé USB. Mais les équipements "qui ne sont pas de confiance" intègrent-ils les bornes d'accès Wi-Fi déployées dans les hôtels ? Là aussi, nous attendons des précisions de la part de l'ANSSI avec laquelle nous avons pris contact.

C'est moins connu mais il faut également se méfier des bornes électriques libre-service si vous cherchez à recharger vos équipements. "Certaines de ces bornes peuvent avoir été conçues pour copier les documents à votre insu", précise le Passeport de conseils aux voyageurs.

Pour sensibiliser les managers de manière plus globale, la délégation interministérielle à l'Intelligence économique (D2IE) a publié en avril dernier un fascicule comprenant 22 fiches pratiques pour la "sécurité économique".

Un exercice louable pour s'adresser de manière pragmatique aux dirigeants de PME ou d'entreprises plus grandes. Mais l'avertissement demeure vague pour les séjours en hôtel : "Être prudent dans les communications : garder à l'esprit que les conversations au téléphone ou par Internet peuvent être interceptées (Wi-Fi des hôtels, etc.)." (voir fiche 17 "Se déplacer à l'étranger").

On ressent un certain décalage entre la présentation globale des risques, qui ne colle pas vraiment avec la menace Darkhotel repérée par Kaspersky. Et on peut regretter dans ces moments que le portail public de la sécurité informatique, inauguré en février 2008, ne soit pas vraiment mis à jour…

—
Quiz : Connaissez-vous les VPN ?
—-

Crédit photo : Shutterstock.com – Droit d'auteur : Mark Rubens