La sécurité des entreprises sous la menace des cybercafés

Le résultat est édifiant. Selon le laboratoire de recherche en cryptologie et virologie opérationnelles (CVO) de l'**Esiea** (école supérieure d'informatique, électronique, automatique), les cybercafés et autres lieux de connexion Internet en libre service (hôtels, gares, aéroport, etc.) constituent **des mines d'or pour les spécialistes de l'espionnage économique**. Ils peuvent notamment y retrouver nombre de documents confidentiels tels que des audits financiers de groupes industriels, des archives de la Haute cour de justice, ou encore des copies d'avis d'imposition et de certificats d'identité. L'étude complète sera dévoilée à l'occasion de la conférence Eciw 2011 en juillet prochain. L'Eisea s'était déjà distinguée il y a un an environ en révélant la faiblesse des antivirus du commerce.

Effectuée pour le compte de **Secalys**, une entreprise spécialisée dans le conseil en sécurité aux entreprises, l'enquête s'est déroulée entre avril et août 2010 dans les principaux cybercafés et points de consultation Internet publics de Paris et ses alentours, mais également dans plusieurs villes de provinces et à l'étranger (Allemagne, Belgique, Grèce, Luxembourg). Côté méthode, les enquêteurs ont utilisé une clé USB dotée de l'application exécutable localement DrWeb qui permet notamment de récupérer les données effacées.

Une méthodologie relativement simple à mettre en oeuvre et, donc, exploitable par n'importe quel utilisateur quelque peu familliié avec les technologies informatiques. Plus grave, l'étude a permis de constater **le faible niveau de protection des terminaux librement accessibles**. *« Il est facile par de nombreux moyens [hors exploitation des failles systèmes] d'acquérir des privilèges systèmes et donc d'installer des codes malveillants qui infecteront les utilisateurs ultérieurs »*, prévient **Eric Filiol**, qui pilote le laboratoire de recherche de l'Esiea, cité par *Les Echos* (01/12) qui révèle l'information.

Un constat d'autant plus alarmant que, selon l'enquête, **les ordinateurs Internet publics ont la préférence des cadres de haut niveau et dirigeants** d'entreprise. Pensant que la connexion wifi de leur ordinateur portable, peut être interceptée (ce qui est vrai sauf si la communication est chiffrée avec un protocole de codage suffisamment élevé type WPA), ils se tournent vers les terminaux Internet en accès libres.

Les espions ne se contentent alors pas de récupérer des documents confidentiels issus des envois éventuels des utilisateurs victimes. Ils tenteront d'introduire un malware sur la clé USB de l'employé afin d'**ouvrir une porte dérobée, à l'aide d'un cheval de Troie, sur le système d'information de l'entreprise** et de s'y introduire. Soit une variante plus sophistiquée des clés USB infectieuses volontairement « perdues » dans les parking des grandes entreprises et autres centres d'affaires. Mais au final, c'est bien la propriété intellectuel et stratégique de l'entreprise qui risque de tomber entre de mauvaises mains.