Les cybercafés sont mal sécurisés selon des experts

- Informatique - Sécurité Informatique -

Date de mise en ligne : lundi 29 novembre 2010

Spyworld Actu

Des spécialistes en sécurité français ont joué les espions. Profitant du manque de sécurité des cybercafés, ils ont mis la main sur nombreux documents confidentiels laissés par les clients.

Pirater un cybercafé, ou le PC en libre-service d'un hôtel, est presque à la portée de tous ! C'est ce que vient de démontrer une équipe du Laboratoire de cryptologie et de virologie opérationnelles de l'ESIEA (Ecole supérieure d'informatique électronique eta utomatique) qui a mené une enquête pour le compte de Secalys, un cabinet spécialisé dans l'intelligence économique et la sécurité.

L'opération a été réalisée à Paris (et dans plusieurs pays européens), d'avril à août 2010, dans une cinquantaine de cybercafés et une vingtaine d'hôtels de trois à cinq étoiles près de gares et d'aéroports. Et ses résultats sont plutôt inquiétants pour la sécurité de ces établissements.

Les chercheurs sont en effet parvenus à récupérer, sans trop de difficulté, plusieurs gigaoctets de documents confidentiels sur les ordinateurs installés : audits financiers de groupes industriels, un document de la haute cour de justice européenne, photocopies d'un avis d'imposition, de passeports et de cartes d'identité... Autant d'informations permettant de récupérer de précieuses informations sur une entreprise ou pour réaliser de faux papiers ou une usurpation d'identité. Certains documents étaient tellement sensibles qu'ils ont été transmis aux autorités compétentes !

Le contrôle total d'un cybercafé

Pour jouer aux espions, l'équipe de l'ESIEA a juste utilisé une clé USB, sur laquelle étaient notamment installés le logiciel de récupération de données effacées PhotoRec, et un keylogger matériel (logiciel espion), accessoire en vente sur Internet. En utilisant ce support amovible, l'intrusion de l'équipe n'a laissé aucune trace.

Simple et efficace, la méthode se déroule en deux étapes. La première consiste à préparer « le terrain ». L'expert place le keylogger au niveau de la prise clavier du PC du cybercafé. Ensuite, il provoque le blocage du PC (simple extinction, plantage avec écran bleu, deni de service...) ce qui déclenche une alarme sur la machine de l'administrateur du cybercafé. Ce dernier intervient aussitôt en entrant son identifiant et mot de passe. Ces deux données sont discrètement récupérées par le keylogger. Seconde étape : l'attaque. De retour dans le cybercafé quelques heures ou jours plus tard, l'expert accède à tous les PC de la boutique grâce à l'identifiant et au mot de passe du gérant (cette étude montre en effet que très peu d'administrateurs ont un identifiant et un mot de passe différents pour chaque machine).

L'expert peut alors faire ce qu'il veut : placer des codes malveillants pour infecter des clés USB de clients, lancer une attaque virale à destination d'une entreprise (ou d'un pays) ou récupérer des documents laissés par les particuliers. « Même si un document n'est stocké que sur la clé du client, on peut le récupérer avec un logiciel capable d'aspirer tout le contenu d'un support amovible », explique Eric Filiol, directeur du laboratoire de l'ESIEA. Les détails techniques et opérationnels de cette étude seront publiés lors de la conférence ECIW (European Conferences on Information Warfare and Security) 2011 à Tallinn en juin prochain.

Post-scriptum :

http://www.01net.com/www.01net.com/...